WatchGuard® System Manager User Guide

WatchGuard System Manager v8.0

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Complete copyright, trademark, patent, and licensing information can be found in the appendix of this User Guide.

Management Software: 8.0
Appliance Software: WFS 7.4 and Fireware Pro 8.0
Document Version: 8.0-050411

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT:
www.watchguard.com/support
support@watchguard.com
U.S. and Canada +877.232.3531
All Other Countries +1.206.613.0456

SALES:
U.S. and Canada +1.800.734.9905
All Other Countries +1.206.521.8340

ABOUT WATCHGUARD

WatchGuard is a leading provider of network security solutions for small- to mid-sized enterprises worldwide, delivering integrated products and services that are robust as well as easy to buy, deploy and manage. The company's Firebox X family of expandable integrated security appliances is designed to be fully upgradeable as an organization grows and to deliver the industry's best combination of security, performance, intuitive interface and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of the security landscape with vulnerability alerts, software updates, expert security instruction and superior customer care. For more information, please call (206) 521-8340 or visit www.watchguard.com.

Contents

CHAPTER 1

Getting Started

Historically, organizations used many tools, systems, and personnel to control the security of their networks. Different computer systems controlled access, authentication, virtual private networking, and network control. These expensive systems are not easy to use together or to keep up-to-date. WatchGuard® System Manager (WSM) supplies an integrated solution to manage your network and control security problems. This chapter tells you how to install WatchGuard System Manager into your network.

About WatchGuard System Manager

WatchGuard® System Manager (WSM) gives you an easy and efficient way to manage your network security. Use one computer as a management station to show, manage, and monitor all the Fireboxes in your network.

WSM gives support for mixed environments. You can manage Firebox® III and Firebox X devices that use different versions of appliance software. You can also manage Firebox X Edge devices.

WSM has three servers that do Firebox management functions:

WatchGuard Management Server

The WatchGuard Management Server operates on a Windows computer. With this server, you can manage all Firewall devices and create VPN tunnels using a simple drag-and-drop function. The basic functions of the Management Server are:

- Centralized management of VPN tunnel configurations
- The certificate authority for distributing certificates for IPSec tunnels
- Protocol translation in support of the WatchGuard SOHO and Firebox X Edge products

Log Server

The Log Server collects logs from each WatchGuard Firebox. The native storage format is XML (plain text) for easy troubleshooting and reporting. Among the information collected from firewall devices are traffic logs, event logs, alarms, and diagnostic messages.

WebBlocker Server

The WebBlocker Server operates with the Firebox HTTP proxy to deny user access to applicable Web sites. The administrator sets the categories of permitted Web sites during

Firebox configuration. The HTTP proxy on the Firebox then works with the WebBlocker Server to find if a Web site is in a category that is not allowed.

About Hardware and Appliance Software

Appliance software is a software program or operating system that is permanently kept on your hardware. The Firebox® uses the appliance software with the configuration file to operate. When you upgrade your Firebox device, you write a new version of the appliance software to its memory. Although each Firebox model is loaded with a default appliance software type, you can upgrade the appliance software independently of the hardware.

Two types of appliance software are available to WatchGuard® customers:

- WatchGuard Firebox System (WFS) — This is the default appliance software on Firebox III and Firebox X Core devices. It is the standard version of the appliance software successfully used by WatchGuard customers since 1998, with several new enhancements added.
- Fireware Pro — This is the default appliance software on Firebox X Peak devices. If you have a Firebox X Core, you can purchase a Fireware upgrade. This software has the following advanced features for more complex networks:
  - Signature-based IDP
  - Gateway AntiVirus for E-Mail
  - Advanced networking options including QoS, dynamic routing, and support for multiple WAN interfaces

When you install WatchGuard System Manager, it automatically installs the software tools you must have to configure and manage a Firebox with any type of appliance software. These include:

- Firebox System Manager
- Policy Manager
- HostWatch

When you add a Firebox to be managed by WSM, the software automatically identifies which appliance software the Firebox uses. If you select the Firebox and then click an icon on the toolbar, it automatically starts the correct management tool.

For example, if you add a Firebox X700 operating with WFS appliance software to the **Devices** tab of WFS and then click the Policy Manager icon on the WSM toolbar, Policy Manager for WFS automatically starts and opens the configuration file. However, if you add a Firebox X700 operating with Fireware appliance software and click the Policy Manager icon, Policy Manager for Fireware starts instead.

Upgrading the appliance software

If you have a Firebox X Core, the WFS appliance software is loaded on the box. Or, you can purchase an upgrade to Fireware Pro. See the *Migration Guide* for information on upgrading from WFS to Fireware Pro.

Installing WatchGuard System Manager

Note

This installation procedure is for new installations only. If you have an earlier version of WatchGuard® System Manager, use the upgrade procedure in the Migration Guide.

WatchGuard System Manager includes firewall appliance software and management software to protect your network from attack. You put the Firebox® between the Internet and your trusted computers. You then use the software installed on the management station to configure and to monitor your Firebox.

To install the WatchGuard System Manager software, you must:

- Collect your network addresses and information
- Select a network configuration mode, if you are using WFS appliance software only. This step is not necessary if you use Fireware appliance software.
- Select to install the Management Server, Log Server, and WebBlocker Server on the same computer as your management software, or on a different computer.
- Configure the management station
- Use the Quick Setup Wizard to make a basic configuration file
- Put the Firebox into operation on your network

Note

This chapter gives the default information for a Firebox with a three-interface configuration. If your Firebox has more interfaces, use the same configuration tools and procedures as the instructions for the optional interface to configure the other interfaces.

Installation requirements

Before you install WatchGuard System Manager, make sure that you have these items:

- WatchGuard Firebox security device
- WatchGuard System Manager CD-ROM
- A serial cable (blue)
- Three crossover Ethernet cables (red)
- Three straight Ethernet cables (green)
- Power cable
- LiveSecurity Service license key

Collecting network information

License Keys

Collect your license key certificates. WatchGuard System Manager comes with a LiveSecurity Service key that enables your subscription to the LiveSecurity service. For more information about this service, see the "Service and Support" chapter in this guide,

You get the license keys for any optional products when you purchase them. For more information about optional products, see the *Configuration Guide* for your version of appliance software.

Network addresses

We recommend that you make two tables when you configure your Firebox. Use the first table for your network IP addresses before you put the Firebox into operation.

WatchGuard uses slash notation to show the subnet mask.

*1*Network IP Addresses Without the Firebox

Wide Area Network	_____._____._____._____ / ____
Default Gateway	_____._____._____._____
Local Area Network	_____._____._____._____ / ____
Secondary Network (if applicable)	_____._____._____._____ / ____
Public Server(s) (if applicable)	_____._____._____._____
	_____._____._____._____
	_____._____._____._____

Use the second table for your network IP addresses after you put the Firebox into operation.

External interface

Connects to the external network (typically the Internet) that is the security problem.

Trusted interface

Connects to the private LAN or internal network that it is necessary to protect.

Optional interface(s)

Usually connects to the DMZ or the mixed trust area of your network. The number of optional interfaces on your Firebox depend on the model you have purchased. Use optional interfaces to create zones in your network with different levels of access. Usually, you install the Web, e-mail, and FTP servers on an optional interface.

*2*Network IP Address With the Firebox

Default Gateway	_____._____._____._____
External Network	_____._____._____._____ / ____
Trusted Network	_____._____._____._____ / ____
Optional Network	_____._____._____._____ / ____
Secondary Network (if applicable)	_____._____._____._____ / ____

Selecting a firewall configuration mode

Fireware appliance software users must use a routed firewall configuration mode. If you use WFS appliance software, you must make a decision on how to install the Firebox into your network before you install WatchGuard System Manager. This decision controls the configuration of the Firebox interfaces. To install the Firebox into your network, select the configuration mode—routed or drop-in—that matches the needs of your current network.

For more information on finding which configuration mode to use with WFS appliance software, see “WFS appliance software configuration modes” on page 9.

Selecting where to install server software

During installation, you can select to install the management station and three WatchGuard System Manager Server components on the same computer. Or you can use the same installation procedure to install the server components on other computers. To decide, you must examine the capacity of your management station and select the installation method that best matches your needs.

If you install the Management Server, Log Server, or WebBlocker Server on a computer with an active desktop firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to change their desktop firewall configuration. See "Installing WatchGuard Servers on computers with desktop firewalls" on page 8 for more information.

Setting up the management station

The management station runs the System Manager software. This software shows the traffic through the firewall. System Manager also shows connection and tunnel status. The WatchGuard Log Server records information it receives from the Firebox. You can get access to this data using tools on the management station.

Select one computer on your network as the management station and install the management software:

1 Insert the WatchGuard System Manager CD-ROM in the CD drive of your computer. If the installation wizard does not appear automatically, double-click `install.exe` in the root directory of the CD.

2 Click **Connect to LiveSecurity** on the WatchGuard System Manager Installation screen. This starts your Web browser and connects your computer to the WatchGuard Web site.
If you do not have an Internet connection, install the software from the CD-ROM. If you use this procedure, you cannot get support, strong encryption, or VPN functions until you enable the LiveSecurity Service.

3 Use the instructions on the screen to start your LiveSecurity Service subscription.

4 Download the WatchGuard System Manager software. The speed of your Internet connection controls the time to download the software.
Make sure that you write down the name and the path of the file when you save it to your hard drive.

5 When the download is complete, open the file and use the instructions on the screens to help you through the installation.
The Setup program includes a screen in which you select the components of the software or the upgrades to install. A different license is necessary when you install some software components.

Note

If your management station is already operating with a Windows toolbar, some users can find it necessary to stop and restart the toolbar before you can see the new toolbar components installed for the WatchGuard Management System.

6 At the end of the installation wizard, a check box appears that you can select to start the Quick Setup Wizard. Make sure you install the cables to your Firebox before you start the Quick Setup Wizard.

Software encryption levels

The management station software is available in two encryption levels.

Base

Uses 40-bit encryption

Strong

Uses 128-bit 3DES encryption

A minimum of 56-bit encryption is necessary for the IPSec standard. To use virtual private networking with IPSec you must download the strong encryption software.

Strong export limits apply to the strong encryption software. It is possible that it is not available for download.

Backing up your previous configuration

If you have an earlier version of WatchGuard System Manager, you must make a backup of your security policy configuration before you install a new version. For instructions on creating a backup of your configuration:

- If you are upgrading to a newer version of the WFS appliance software, refer to the *Upgrade Guide*.
- If you are moving from WFS to Fireware appliance software, refer to the *Migration Guide*.

Using the Quick Setup Wizard

After you configure the management station, install the Firebox cables, and (if applicable) make a back up of your previous configuration, use the Quick Setup Wizard to make a basic configuration file. The Firebox uses this basic configuration file when it starts for the first time. This enables the Firebox to operate as a basic firewall.

After the Firebox is configured with this basic configuration, you can use Policy Manager to expand or change the Firebox configuration.

The Quick Setup Wizard uses a device discovery procedure to find the Firebox X model you are configuring. This procedure uses a UDP broadcast. Software firewalls, including the firewall in Microsoft Windows XP SP2, can cause problems with the discovery procedure.

You can start the Quick Setup Wizard from the Windows desktop or from System Manager. The instructions in the wizard help you through the procedure.

From the desktop, select **Start > Programs > WatchGuard System Manager 8 > Quick Setup Wizard**. Or, from System Manager, select **Resources > Quick Setup Wizard**.

Putting the Firebox into operation on your network

You have completed the installation of your Firebox. You can use the Firebox as a basic firewall that allows all outgoing traffic.

Complete these steps to put the Firebox into operation on your network:

- Put the Firebox in its permanent physical location.
- In WatchGuard System Manager, use **File > Connect To** to connect the management station to the Firebox.
- If you use a routed configuration, change the default gateway on all computers that you connect to the Firebox trusted IP address.
- Configure the Log Server to start recording log messages.
- Open Policy Manager to change the basic configuration to meet your security needs.

Setting Up Your Management Server

You can select to install the Management Server on the your management station during installation. Or, you can use the same installation procedure to install the Management Server on a different computer. You must install the Management Server software on a computer that is behind a Firebox with a static external IP address. The Management Server does not operate correctly if it is behind a Firebox with a dynamic IP address on its external interface.

You use this server to:

- Start and stop the Management Server
- Set the server passphrases and license key

- Set the CRL distribution point and publication period
- Set the client and root certificate lifetime
- Launch the CA Web GUI

For information on how to set up the other WatchGuard System Manager servers—Log Server and WebBlocker server, see the "Working with Log Files" chapter in this guide, and the *Configuration Guide*, respectively.

Note

If you install the Management Server, Log Server, or WebBlocker Server on a computer with an active desktop firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to change their configuration. See the section "Installing WatchGuard Servers on computers with desktop firewalls" on page 8 for more information.

Management Server passwords

The WatchGuard Management Server uses passwords to protect sensitive information kept on disk or to secure communications with client systems.

Master password

This password is used to protect all the passwords that are kept in the password file. You must use it when you move the Management Server data to a new system or when you restore a lost or corrupt master key file. Because you do not frequently use the master password, we recommend that you write it down and lock it in a secure location.

The master password is not stored in the password file. An encryption key is derived from the master password and the key data is kept on disk. The default locations for the password file and encryption key are:

- C:\Documents and Settings\WatchGuard\wgauth\wgauth.ini
- C:\Documents and Settings\WatchGuard\wgauth\wgauth.key

Because these files are used by the Management Server software, you must never change them manually.

Admin password

The administrator uses the admin password frequently because it is necessary to use it to connect to the Management Server using WatchGuard System Manager.

Using the Management Server Setup Wizard

1 Right-click the Management Server icon in the WatchGuard toolbar at the bottom of the screen.

2 Select **Start Service**.

The Management Server setup wizard starts. The instructions in the wizard help you through the procedure.

Note the following:

- When an interface whose IP address is bound to the Management Server goes down and then restarts, we recommend that you restart the Management Server.
- If you change the computer's IP address, you must remove the Management Server and install it again.

After Your Installation

You have satisfactorily installed, configured, and put your new WatchGuard® System Manager into operation on your network. Here is some more information to think about.

Align your security policy

Your security policy controls who can get in to your network, where they can go, and who can get out. The configuration file of your Firebox® makes the security policy.

The configuration file that you make with the Quick Setup Wizard is only a basic configuration. You can make a configuration file that aligns your security policy with your requirements. To do this, add filtered and proxied policies, in addition to the basic policies you are told about in the sections before. These policies expand what you let in and out of your network. Each policy can have an effect on your network. The policies that increase your network security can decrease access to your network. The policies that increase access to your network can decrease your network security. When you select these policies, you must select a range of balanced policies. Your organization and the computer equipment to which you give protection will control your selection. Some policies that organizations usually add are HTTP and SMTP. Usually, for a new installation, we recommend that you use only packet filter policies until all your systems operate correctly. Then, as necessary, you can add proxied policies when you know more about them.

For more information about policies, see the *Configuration Guide* for your version of appliance software.

Features of the LiveSecurity Service

Your Firebox includes a subscription to our LiveSecurity® Service. Your subscription:

- Makes sure that you get the newest network protection with the newest software upgrades
- Gives solutions to your problems with full technical support resources
- Prevents downtime with messages and configuration help to prevent the newest network security problems
- Helps you to find out more about network security through training resources
- Extends your network security with included software and other features

Installation Topics

The following sections give information that you can use while setting up your Firebox®.

Installing WatchGuard Servers on computers with desktop firewalls

Desktop firewalls can block the ports necessary for WatchGuard® Server components to operate. Before installing the Management Server, Log Server, or WebBlocker Server on a computer with an active desktop firewall, other than Windows Firewall, you might need to open the necessary ports on the desktop firewall. Windows Firewall users do not need to change their configuration.

This table shows you the ports you must open on a desktop firewall.

Server Type/Appliance Software	Protocol/Port
Management Server	TCP 4109, TCP 4110, TCP 4112, TCP 4113
Log Server with Fireware appliance software with WFS appliance software	 TCP 4115 TCP 4107
WebBlocker Server	TCP 5003, UDP 5003

WFS appliance software configuration modes

There are two configuration modes available for users with WFS appliance software: a routed configuration or a drop-in configuration. (If you are using Fireware appliance software, drop-in mode is not available.) Many networks operate the best with a routed configuration. But we recommend the drop-in mode if:

- You have a large number of public IP addresses
- You have a static external IP address
- You cannot configure the computers on your trusted and optional networks that have public IP addresses with private IP addresses

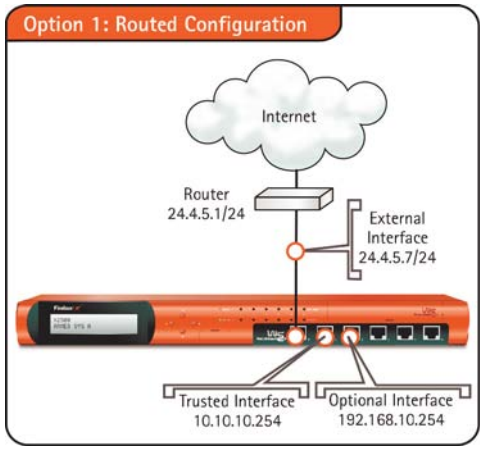
The table below shows three conditions that can help you to select a firewall configuration mode. We then give more information about each mode.

	Routed Configuration	Drop-in Configuration
Condition 1	All interfaces of the Firebox are on different networks. The minimum configured interfaces are external and trusted.	All interfaces of the Firebox are on the same network and have the same IP address (Proxy ARP).
Condition 2	Trusted and optional interfaces must be on different networks. The two interfaces must have an IP address on their respective network.	The computers on the trusted or optional interfaces can have a public IP address.
Condition 3	Use static NAT to map public addresses to private addresses behind the trusted or optional interfaces.	The machines that have public access have public IP addresses. Thus, no static NAT is necessary.

Routed configuration

You use the routed configuration when you have a small number of public IP addresses or when your Firebox gets its external IP address using PPPoE or DHCP. This configuration also makes it easier to configure virtual private networks.

In a routed configuration, you install the Firebox with different logical networks and network addresses on each of its interfaces. The public servers behind the Firebox use private IP addresses. The Firebox uses network address translation (NAT) to route traffic from the external network to the public servers.

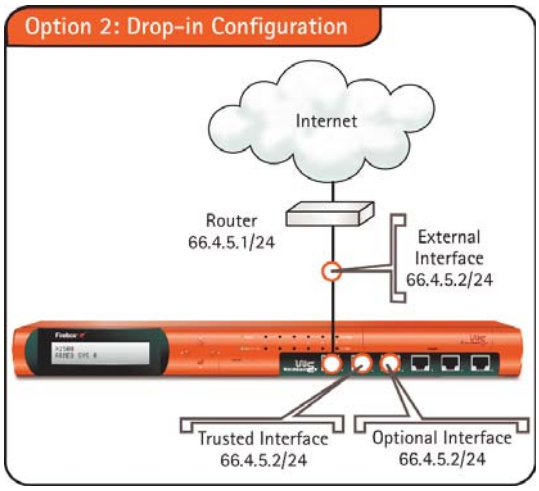


The requirements for a routed configuration are:

- All interfaces of the Firebox must be on different logical networks. The minimum configuration includes the external and trusted interfaces. You can also configure one or more optional interfaces.
- All computers behind the trusted and optional interfaces must have an IP address from that network. For example, a computer on a trusted interface in the previous figure could have an IP address of 10.10.10.200 but not 192.168.10.200, which is on the optional interface.

Drop-in configuration

With a drop-in configuration, the Firebox uses the same network for all of its interfaces. You must configure all of the interfaces. When you install the Firebox between the router and the LAN, it is not necessary to change the configuration of the local computers. The public servers behind the Firebox continue to use public IP addresses. The Firebox does not use network address translation to route traffic from the external to your public servers.



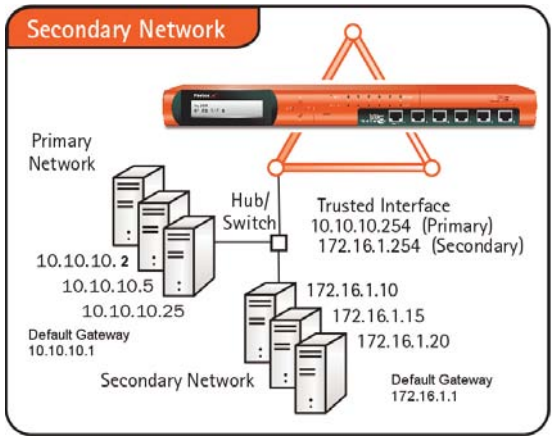
The properties of a drop-in configuration are:

- You use one logical network for all three interfaces.
- The Firebox uses proxy ARP. The trusted interface ARP address replaces the ARP address of the router. It then resolves the ARP data for those devices behind the Firebox that cannot receive the transmitted data.
- During installation, it is not necessary to change the TCP/IP properties of computers on the trusted and optional interfaces. The router cannot receive the transmitted ARP data from the trusted host, but the Firebox continues to control ARP data for the router.
- Usually, the Firebox is the default gateway as an alternative to the router.
- You must flush the ARP cache of each computer on the trusted network.
- A large part of a LAN is on the trusted interface because there is a secondary network for the LAN.

With a drop-in configuration you do not have to change the configuration of each computer on the trusted network that has a public IP address. But, a drop-in configuration is not easy to manage. It can also be more difficult to troubleshoot problems.

Adding secondary networks to your configuration

A secondary network is a different network that connects to a Firebox interface with a switch or hub.



When you add a secondary network, you map an IP address from the secondary network to the IP address of the Firebox interface. Thus, you make (or add) an IP alias to the network interface. This IP alias is the default gateway for all the computers on the secondary network. The secondary network also tells the Firebox that there is one more network on the Firebox interface.

To add a secondary networks, do one of these procedures:

Use the Quick Setup Wizard during installation

Enter an IP address for the secondary network in the Quick Setup Wizard, as described in “Using the Quick Setup Wizard” on page 6. This is the default gateway for your secondary private network.

Add the secondary network after the Firebox installation is complete

Use Policy Manager to add secondary networks to an interface. For information on how to use Policy Manager, see the *Configuration Guide*.

Dynamic IP support on the external interface

If you use dynamic IP addressing, you must select routed configuration.

If you select the Dynamic Host Configuration Protocol (DHCP), the Firebox tells a DHCP server controlled by your Internet Service Provider (ISP) to give the Firebox its IP address, gateway, and netmask. This server can also give WINS and DNS server information for your Firebox. If it does not give you that information, you must add it manually to your configuration. If necessary, you can change the WINS and DNS values that your ISP gives you.

Point-to-Point Protocol over Ethernet (PPPoE) is also available. As with DHCP, the Firebox makes a PPPoE protocol connection to the PPPoE server of your ISP. This connection automatically configures your IP address, gateway, and netmask. But, PPPoE does not supply you with DNS and WINS server information as DHCP does.

If you use PPPoE on the external interface, you must have the PPP user name and password when you configure your network. The user name and password each have a 256-byte capacity.

When you configure the Firebox to receive dynamic IP addresses, the Firebox cannot use these functions (for which a static IP address is necessary):

- High Availability (not available on Firebox 500)
- Drop-in mode (if you are using WFS appliance software)
- 1-to-1 NAT
- MUVPN
- RUVPN with PPTP

Note

If your ISP uses a DHCP or PPPoE connection to give out static IP address, the Firebox will allow you to enable MUVPN and RUVPN with PPTP because the IP address is static.

External aliases and 1-to-1 NAT are not available when the Firebox is a PPPoE client.

Entering IP addresses

When you enter IP addresses in the Quick Setup Wizard or WSM dialog boxes, type the digits and periods in the correct sequence. Do not use the TAB key, arrow key, spacebar, or mouse to put your cursor after the periods. For example, if you type the IP address 172.16.1.10, do not type a space after you type "16." Do not try to put your cursor after the subsequent period to type "1." Type a period directly after "16," and then type "1.10." Push the slash (/) key to move to the netmask.

About slash notation

Use slash notation to enter the netmask. In slash notation, one number shows how many bits of the IP address identify the network that the host is on. A netmask of 255.255.255.0 has a slash equivalent of 8+8+8=24. For example, an IP address 192.168.42.23/24 is equivalent to an IP address of 192.168.42.23 with a netmask of 255.255.255.0.

This table shows the network masks and their slash equivalents:

Network mask	Slash equivalent
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26

255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Installing the Firebox cables

Connect the power cable to the Firebox power input and to a power source.

The Quick Setup Wizard recommends that you use a straight ethernet cable (green) to connect your management station to a hub or switch. Use another straight ethernet cable (green) to connect your Firebox to the same hub or switch. Then, use the instructions in the Quick Setup Wizard to connect to the Firebox.

You can also use a red crossover cable to connect the Firebox trusted interface to the management station Ethernet port.

CHAPTER 2

Service and Support

No Internet security solution is complete without regular updates and security information. New threats appear each day — from the newest hacker to the newest bug in an operating system — and each can cause damage to your network systems. The LiveSecurity® Service sends security solutions directly to you to keep your security system in the best condition. Training and technical support are available on the WatchGuard® Web site to help you learn more about network security and your WatchGuard products.

LiveSecurity Service Solutions

The number of new security problems and the volume of information about network security continues to increase. We know that a firewall is only the first component in a full security solution. The WatchGuard® Rapid Response Team is a dedicated group of network security personnel who can help you to control this problem of too much information. They monitor the Internet security Web sites for you, to identify new security problems as they start.

Threat responses, alerts, and expert advice

After a new threat is identified, the WatchGuard Rapid Response Team sends you an e-mail to tell you about the problem. Each message gives full information about the type of security problem and the procedure you must use to make sure that your network is safe from attack.

Easy software updates

LiveSecurity® Service saves you time because you receive an e-mail when we release a new version of the WatchGuard System Manager software. Installation wizards, release notes, and a link to the software update make for a fast and easy installation. These continued updates make sure that you do not have to use your time to find new software.

Access to technical support and training

You can find information about your WatchGuard products quickly with our many online resources. You can also speak directly to one of the WatchGuard technical support personnel. Use our online training to learn more about the WatchGuard System Manager software, Firebox, and network security.

LiveSecurity Service Broadcasts

The WatchGuard® Rapid Response Team regularly sends messages and software information directly to your computer desktop by e-mail. We divide the messages into categories to help you to identify and make use of incoming information immediately.

Information Alert

Information Alerts give you a fast view of the newest information and threats to Internet security. The WatchGuard Rapid Response Team frequently recommends that you make a security policy change to protect against the new threat. When necessary, the Information Alert includes instructions on the procedure.

Threat Response

If a new security threat makes it necessary, the WatchGuard Rapid Response Team transmits a software update for your Firebox®. The Threat Response includes information about the security threat and instructions on how to download a software update and install it on your Firebox and management station.

Software Update

When necessary, WatchGuard updates the WatchGuard System Manager software. Product upgrades can include new features and patches. When we release a software update, you get an e-mail with instructions on how to download and install your upgrade.

Editorial

Each week, top network security personnel come together with the WatchGuard Rapid Response Team to write about network security. This continuous supply of information can help you to keep your network safe and secure.

Foundations

The WatchGuard Rapid Response Team also writes information specially for security administrators, employees, and other personnel that are new to this technology.

Loopback

At the end of each month LiveSecurity® Service sends you an e-mail with a summary of the information sent that month.

Support Flash

These short training messages can help you to operate WatchGuard System Manager. They are an added resource to the other online resources:

- Online Help
- FAQs
- Known Issues pages on the Technical Support Web site

Virus Alert

WatchGuard has come together with antivirus vendor McAfee to give you the most current information about computer viruses. Each week, we send you a message with a summary of the virus traffic on the Internet. When a hacker releases a dangerous virus on the Internet, we send a special virus alert to help you protect your network.

New from WatchGuard

When WatchGuard releases a new product, we first tell you — our customers. You can learn more about new features and services, product upgrades, hardware releases, and customer promotions.

Activating the LiveSecurity Service

You can activate the LiveSecurity® Service through the Quick Setup Wizard on the CD-ROM. Or, you can activate it through the activation section of the LiveSecurity Web pages. There is information about the Quick Setup Wizard in the QuickStart Guide and in the "Getting Started" chapter of this book.

Note

To activate the LiveSecurity Service, you must enable JavaScript on your browser.

To activate the LiveSecurity Service through the Web:

1 Make sure that you have the LiveSecurity license key and the Firebox serial number. These are necessary during the LiveSecurity activation procedure.
   - You can find the Firebox serial number in two locations. First, on a small silver label on the outer side of the Firebox package. Second, on a label on the rear side of the Firebox, below the Universal Product Code (UPC) symbol.
   - The license key number is on the WatchGuard LiveSecurity License Key certificate. Make sure that you type it the same as it is shown on the key. Include the hyphens.

2 Using your Web browser, go to:
www.watchguard.com/account/register.asp
The Account page appears.

3 Complete the LiveSecurity Activation page. Use the TAB key or the mouse to move through the fields on the page.
You must complete all the fields to activate correctly. This information helps WatchGuard to send you the information and software updates that are applicable to your products.

4 Make sure that your e-mail address is correct. After you complete the procedure, you get an e-mail message that tells you that you activated the LiveSecurity Service satisfactorily. All your LiveSecurity e-mail will come to this address.

5 Click **Register**.

LiveSecurity Service Self Help Tools

Online Self Help Tools enable you to get the best performance from your WatchGuard® products.

Note

You must activate the LiveSecurity® Service before you can access online resources.

Basic FAQs

The Basic FAQs (frequently asked questions) give general information about the Firebox® and the WatchGuard System Manager software. They are written for the customer who is new to network security and to WatchGuard products.

Advanced FAQs

The Advanced FAQs (frequently asked questions) give you important information about configuration options and operation of systems or products. They add to the information you can find in this User Guide and in the Online Help system.

Known Issues

We know that software products can have bugs. We keep a list of Known Issues to help you find and to configure around these problems in our products until a software update repairs them.

Interactive Support Forum

The WatchGuard Technical Support team operates a Web site where our customers can send messages about WatchGuard products. Technical Support monitors this Web site and writes messages when it is necessary to answer customer problems.

Online Training

Browse to the online training section to learn more about network security and WatchGuard products. You can read training materials and get a certification in our products. The training includes links to a wide range of documents and Web sites about network security. The training is divided into parts which lets you use only the materials you feel necessary. To learn more about online training, browse to:

www.watchguard.com/training/courses_online.asp

Learn About

This is a list of all resources available for a specified product or feature. It is a site map for the feature.

Online Help

There is a copy of the online help system for all WatchGuard products on our Technical Support Web site. You install a copy of the online help when you install WatchGuard System Manager software. The version of online help on our Web site is the most current and includes corrections of errors we find.

Product Documentation

We keep a copy of each user guide we release to customers on our Web site. This includes user guides for versions of software which we do not continue to give technical support. The user guides are in PDF format.

General Firebox X Edge and Firebox SOHO Resources

This section of our Web site shows basic information and links for Firebox X Edge and Firebox SOHO customers. It can help you to install and use the Firebox X Edge and SOHO 6 hardware.

To get access to the LiveSecurity Service Self Help Tools:

1. Start your Web browser. In the address bar, type:
   www.watchguard.com
2. Click **Support**.
3. Log in to the LiveSecurity Service.
4. In the **Self Help Tools** section, click your selection.

WatchGuard Users Forum

The WatchGuard® Users Forum is an online group. It lets the users of WatchGuard products interchange ideas, questions, and information about the product, for example:

- Configuration
- Connecting WatchGuard products and those of other companies
- Network policies

This forum has different categories that you can use to look for information. The WatchGuard Technical Support team controls the forum during regular work hours. Do not use the forum to tell the WatchGuard Technical Support team about problems you have with your Firebox®. You must use the Web interface or the telephone to tell WatchGuard Technical Support directly.

Using the WatchGuard Users Forum

To use the WatchGuard Users Forum you must first create an account:

1 Browse to: www.watchguard.com. Click **Support**. Log in to the LiveSecurity Service.

2 Below **Self Help Tools**, click **Interactive Support Forum**.

3 Click **Create a User Forum account**.

4 Type your information in the page. Click **Create**.
You must select a user name and password. They must be different from the user name and password for your LiveSecurity Service.

WatchGuard Users Group

The WatchGuard® Users Group is an e-mail discussion list. It lets the users of WatchGuard products send and receive messages from other users. Because WatchGuard does not control the group, you cannot use the group to tell the WatchGuard Technical Support team about problems you have with your Firebox®. You must use the Web interface or the telephone to tell WatchGuard Technical Support directly. To learn more about the WatchGuard Users Group, browse to:

lists.watchguard.com/mailman/listinfo/wg-users

Online Help

WatchGuard® Online Help is a Web system that can operate on most computer operating systems. We release each version of our software products with a full online help system. You can find these online help systems at:

www.watchguard.com/help

A static version of the online help system is installed automatically with the WatchGuard System Manager software. You can find it in a subdirectory of the installation folder with the name `Help`. The live version of the online help on the Web site includes corrections to all errors found since we released the software.

Starting WatchGuard Online Help

There are two methods to start the online help system:

- From the WatchGuard System Manager software, press **F1**. Your browser opens and an Online Help page appears. The page has information about the feature you are using.

- Use Windows Explorer or the **Run** command to open the WatchGuard installation folder. Open the **Help** folder. Double-click WFSHelp.htm. Your browser opens and the Online Help home page appears. The default folder is:

C:\Program Files\WatchGuard\Help

Searching for information

There are three methods to search for information in the WatchGuard Online Help system:

Contents

The **Contents** tab shows a list of categories in the help system. Double-click a book to expand a category. Click a page title to look at the contents of that category.

Index

The index shows a list of the words that are in the help system. Type the word, and the list automatically goes to those words that start with the typed letters. Click a page title to look at the contents.

Search

The Search feature is a full text search of the help system. Type a word and press ENTER. A list shows the categories that contain the word. The Search feature does not operate with AND, OR, or NOT operators.

Copy the online help system to more computers

You can copy WatchGuard Online Help from the management station to a second computer. When you do this, copy the full online help folder from the WatchGuard installation directory on the management station. You must include all subdirectories.

Software requirements

- Internet Explorer 4.0 or a subsequent version
- Netscape Navigator 4.7 or a subsequent version

Operating system

- Windows NT 4.0, Windows 2000, or Windows XP
- Sun Solaris
- Linux

Product Documentation

We copy all the user guides we release to our Web site at:

www.watchguard.com/help/documentation/

Technical Support

Your LiveSecurity Service subscription includes technical support for the WatchGuard® System Manager software and Firebox® hardware. To learn more about WatchGuard Technical Support, browse to the WatchGuard Web site at:

www.watchguard.com/support

Note

You must activate the LiveSecurity Service before you can get technical support.

LiveSecurity Service Technical Support

All new Firebox products include the WatchGuard LiveSecurity® Technical Support Service. You can speak with the WatchGuard Technical Support team when you have a problem with the installation, management, or configuration of your Firebox.

Hours

WatchGuard LiveSecurity Technical Support operates from 6:00 AM to 6:00 PM in your local time zone, Monday through Friday.

Telephone Number

877.232.3531 in United States and Canada
+1.206.613.0456 in all other countries

Web Site

http://www.watchguard.com/support

Service Time

We try to supply a solution in a maximum time of four hours.

Type of Service

There is technical support available for special problems with the installation and continued maintenance of the Firebox and SOHO systems.

Single Incident Priority Response Upgrade (SIPRU) and Single Incident After Hours Upgrade (SIAU) are also available. For more data about these upgrades, refer to the WatchGuard Web site at:

http://www.watchguard.com/support

LiveSecurity Gold

WatchGuard Gold LiveSecurity Technical Support adds to your standard LiveSecurity Service. We recommend that you buy this upgrade if your company uses the Internet or VPN tunnels for most of your work.

With WatchGuard Gold LiveSecurity Technical Support you get:

- Live technical support 24 hours a day, seven days a week.
- The Priority Technical Support Team operates our support center continuously from 7 PM Sunday to 7 PM Friday (Pacific Time).
- We try to supply a solution to your problem in a maximum time of one hour.
- If a technician is not immediately available to help you, an administrator records your problem. The administrator gives you an incident number. The Priority Technical Support team will speak to you when they become available.

Firebox Installation Service

WatchGuard Remote Firebox Installation Service helps you to install and configure your Firebox. You can schedule a two-hour time with one of our WatchGuard Technical Support team. During this time, the technician helps you to:

- Do an analysis of your network and security policy
- Install the WatchGuard System Manager software and Firebox hardware
- Align your configuration with your company security policy

This service does not include VPN installation.

VPN Installation Service

WatchGuard Remote VPN Installation Service helps you through a full VPN installation. You can schedule a two-hour time with one of the WatchGuard Technical Support team. During this time, the technician helps you to:

- Do an analysis of your VPN policy
- Configure your VPN tunnels
- Do a test of your VPN configuration

You can use this service after you correctly install and configure your Fireboxes.

Training and Certification

WatchGuard® product training is available online to help you learn more about network security and WatchGuard products. You can find training materials on our Technical Support Web site and prepare for a certification exam. The training materials include links to books and Web sites with more information about network security.

WatchGuard product training is also available at a location near you through a large group of WatchGuard Certified Training Partners (WCTPs). Training partners give training using certified training materials and with WatchGuard hardware. You can install and configure our products with an advanced instructor and system administrator to help you learn.

CHAPTER 3

Monitoring Your Network

To monitor a network, you must have real-time information on all the components of the network. The current status of all VPN devices and tunnels appears in the WatchGuard® System Manager window. You can use these tools to quickly find and troubleshoot problems with your network.

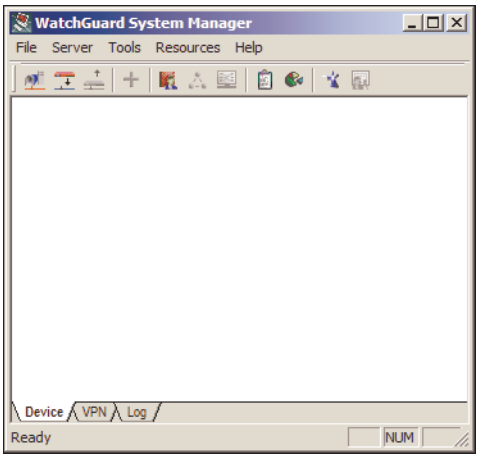
This chapter describes the procedures you can do directly from the WatchGuard System Manager window.

Starting WatchGuard System Manager

From the Windows Desktop:

- Select **Start** > **Programs** > WatchGuard® System Manager 8 > **WatchGuard System Manager**.

The WatchGuard System Manager window appears.



About the WatchGuard System Manager Window

The WatchGuard® System Manager window has three tabs at the bottom of the screen:

Device

A status page for all the devices in System Manager. The information that appears includes the log host, MAC address, and IP address for the interfaces for each device. It also includes the status of all VPN tunnels that are configured in System Manager.

VPN

Shows status information, endpoints, and security parameters for any VPN tunnels created and managed with the WatchGuard Management Server.

Log

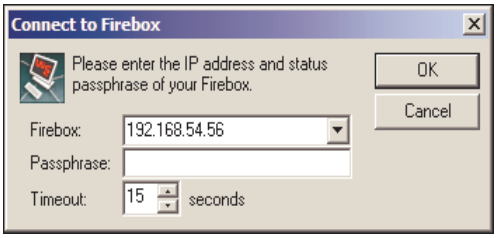
Shows the log status for devices managed by System Manager.

The WatchGuard System Manager window also has menus and icons you can use to start other tools, as described in "Starting Security Applications" on page 29.

Connecting to a Firebox

1 Select **File > Connect to > Device**.

or
Click the **Connect to Device** icon on the WatchGuard® System Manager toolbar. The icon is shown at left.



2 From the **Firebox** drop-down list, select a Firebox® by its IP address or host name.
You can also type the IP address or host name. When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow key.

3 Type the Firebox status (read-only) passphrase.
Use the status passphrase to monitor traffic and Firebox condition. You must use the configuration passphrase to save a new configuration to the Firebox.

4 If necessary, change the value in the **Timeout** field. This value sets the time (in seconds) that the management station listens for data from the Firebox, before it sends a message that shows that it cannot get data from the device.
If you have a slow network or Internet connection to the device, you can increase the timeout value. Decreasing the value decreases the time you must wait for a timeout message if you are connecting to a Firebox that is not accessible.

5 Click **OK**. The Firebox appears in the WatchGuard System Manager window.

Disconnecting from a Firebox

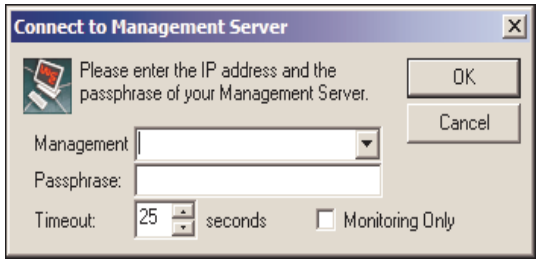
To disconnect, click on the first line of information for the Firebox to disconnect from and select **File > Disconnect**. Or select the Firebox and then click the Disconnect icon shown at left.

Connecting to a Server

The WatchGuard® Management Server (previously the WatchGuard DVCP server) runs on a Windows computer. This computer can be the same one where the WatchGuard management software is installed or a different computer.

1 Select **File > Connect to > Server**.

or
Click the **Connect to Server** icon on the WatchGuard System Manager toolbar. The icon is shown at left.



2 From the **Management** drop-down list, select a server by its host name or IP address.
You can also type the IP address or host name.
When you type an IP address, type all the numbers and the stops. Do not use the TAB or arrow key.

3 Type the password for the Management Server.

4 If necessary, change the value in the **Timeout** field. This value sets the time (in seconds) that the management station listens for data from the Management Server, before it sends a message that shows that it cannot get data from the device.
If you have a slow network or Internet connection to the device, you can increase the timeout value. Decreasing the value decreases the time you must wait for a timeout message if you are connecting to a Management Server that is not accessible.

5 If you are using the server only to monitor traffic, select the **Monitoring Only** check box.

6 Click **OK**.
The server appears in the WatchGuard System Manager window.

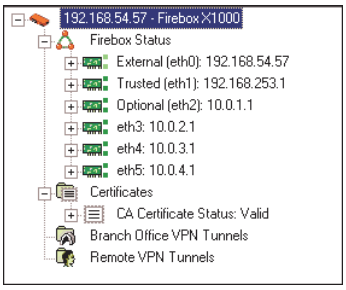
Disconnecting from a Server

To disconnect, click on the Management Server name and select **File > Disconnect**. Or select the Management Server and then click the Disconnect icon shown at left.

Seeing Information about Devices

After you connect to a Firebox or Management Server, information about the devices in your network appears in the WatchGuard® System Manager window.

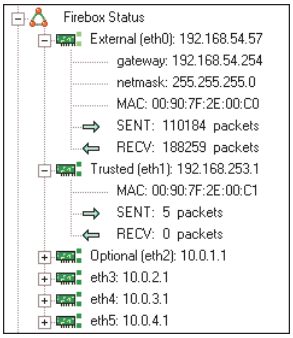
To expand a part of the display, click the plus sign (+) adjacent to the entry, or double-click the name of the entry. To close a part, click the minus sign (–) adjacent to the entry. When no plus or minus sign appears, no more information is available.



Firebox Status

Below Firebox® Status, you can see the IP address and subnet mask of each Firebox interface. If you expand the entries for each interface, you see:

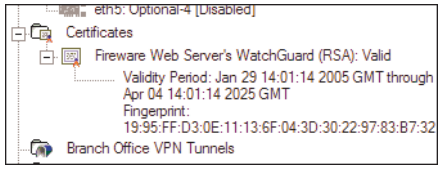
- For the external interface) IP address and netmask of the default gateway.



- Media Access Control (MAC) address of the interface.
- Number of packets sent and received on each interface since the last Firebox restart.

Certificates

Below Firebox Status, you can see the status, the interval of time that the certificate is valid, and the fingerprint of CA and IPSec certificates.



Branch Office VPN Tunnels

Below the Firebox Status is a section on branch office virtual private network (BOVPN) tunnels. There are two types of IPSec BOVPN tunnels: VPN tunnels built manually using Policy Manager and VPN tunnels built using the Management Server.

An expanded entry for a BOVPN tunnel shows the following information:

- The tunnel name, the IP address of the destination IPSec device (a different Firebox, Edge, SOHO, or SOHO|tc), and the tunnel type. If the tunnel is managed by the Management Server, the IP address refers to the full remote network address.
- The volume of data sent and received on the tunnel in bytes and packets.
- The time before the key expires and when the tunnel is created again. This appears as a time limit or as the volume of bytes. If you use the Management Server to configure a tunnel to expire using time and volume limits, the two expiration values appear.
- Authentication and encryption layers set for the tunnel.
- Routing policies for the tunnel.

Mobile user VPN tunnels

After the branch office VPN tunnels list is an entry for Mobile User VPN tunnels. The entry shows the same information as for Branch Office VPN. This includes the tunnel name, the destination IP address, and the tunnel type. Packet information, the key expiration date, authentication, and encryption data also appear.

PPTP user VPN tunnels

For PPTP RUVPN tunnels, the WatchGuard System Manager shows only the quantity of sent and received packets. The volume of bytes and total volume of bytes are not applicable to PPTP tunnels.

Connection status

The tree view for each device shows a red, yellow, or no exclamation point. The exclamation point shows whether the WSM is receiving status information from the device. The status descriptions are as follows:

No exclamation point

Usual operation. The device is successfully sending data to WatchGuard System Manager.

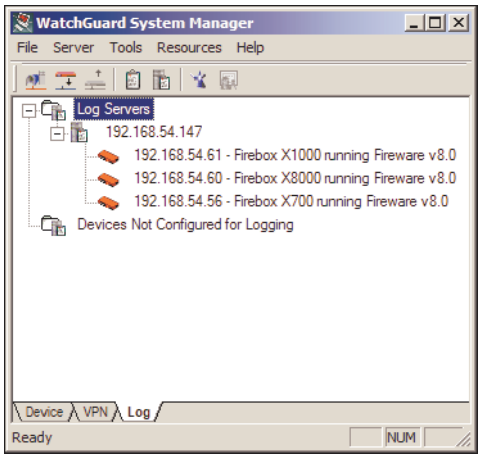
Red exclamation point

Problem. The device cannot send or receive traffic with the management station at this time.

Seeing Information on Log Servers

Click the **Log** tab to see a list of log servers managed by WatchGuard® System Manager. The list of servers in use is collected from the configuration files of the devices that are monitored. The display also shows

devices for which logging is not configured. Logging for devices is configured in Policy Manager, as described in the *Configuration Guide* for your appliance software.



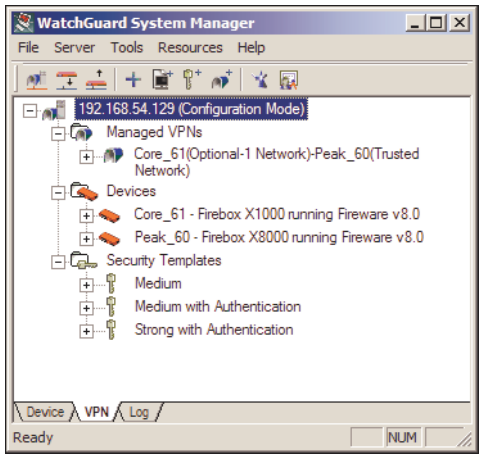
Monitoring VPNs

The VPN tab shows all Fireboxes that the Management Server is managing. The configured VPN information for each Firebox is also shown here.

Fireboxes that you connect to manually using WatchGuard System Manager do not appear here. VPN policies that you create manually with Policy Manager are also not shown here.

All devices appear in a tree view structure. When the text box adjacent to an entry contains a plus sign (+), the tree is closed. To expand it, click the plus sign. The tree view expands at that entry to show the properties of that device.

To close the display, click the minus sign (–) adjacent to a device. The expanded tree closes, and keeps a single-line entry for that device.

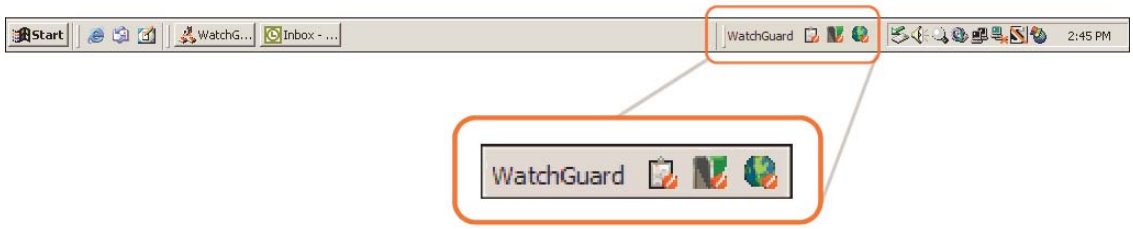


About the WatchGuard Toolbar

There are three servers that do Firebox® management functions:

- Management Server
- Log Server
- WebBlocker Server

You start, stop, and configure these Management Servers using the WatchGuard® toolbar. The WatchGuard toolbar is one of the toolbars at the bottom of your computer screen.



From left to right, the icons on the toolbar manage these servers:

- Log Server — This server collects log messages, event messages, alarms, and diagnostic messages from Firebox X Edge, WFS, and Fireware-based devices. The native storage format is XML (plain text). For information on Log Server, see the chapter "Reviewing and Working with Log Files" in this guide.
- Management Server — The WatchGuard Management Server (previously the WatchGuard DVCP server) runs on a Windows computer. This computer can be the same one where the WatchGuard management software is installed or a different computer. There are tools included to help with the migration of a DVCP server from a Firebox to your computer. For information on using this wizard, see the "Getting Started" chapter in this guide.
- WebBlocker Server — This server works with the Firebox HTTP proxy to restrict user access to particular web sites. For information on WebBlocker, see the configuration guide for your appliance software.

Starting Security Applications

You can start the following tools from WatchGuard® System Manager using the icons on the taskbar and menu options:

Policy Manager

Policy Manager lets you install, configure, and customize a network security policy. For information on using Policy Manager, see the *Configuration Guide* for your appliance software.

To configure or customize the security policy of a Firebox X Edge or Firebox SOHO, you must use the web user interface to connect to the device.

Firebox Manager

WatchGuard Firebox® System Manager lets you start many different security tools in one easy to use interface. You can also use Firebox System Manager to monitor real-time traffic

through the firewall. For information on using Firebox System Manager, see the *Configuration Guide* for your appliance software.

HostWatch

HostWatch shows the connections through a Firebox from the trusted network to the external network. It shows the current connections, or it can show the connections from a list in a log file. For information on using HostWatch, see the Configuration Guide for your appliance software.

Log Viewer

Log Viewer shows a static view of a log file. It lets you:

- Apply a filter by data type
- Search for words and fields
- Print and save to a file

For information on using Log Viewer, see the chapter "Reviewing and Working with Log Files" in this guide.

Historical Reports

These HTML reports give data to use when you monitor or troubleshoot the network. The data can include:

- Type of session
- Most active hosts
- Most used services
- URLs

For information on using Historical Reports, see the chapter "Generating Reports of Network Activity" in this guide.

Quick Setup Wizard

The Quick Setup Wizard helps you to quickly set up a basic configuration for a Firebox.

CHAPTER 4

Setting Up Logging and Notification

An event is any single activity that occurs at the Firebox®, such as denying a packet from passing through the Firebox. Logging is the recording of these events to a log host. A notification is a message sent to the administrator by the Firebox when an event occurs that indicates a security threat. Notification can be in the form of e-mail or a pop-up window.

For example, WatchGuard® recommends that you configure default packet handling to issue a notification when the Firebox finds a port space probe. When this occurs, the log host sends notification to the network security administrator about the rejected packets. The network security administrator can examine the log files and make decisions about how to add more security to the organization's network. Some possible changes are:

- Block the ports on which the probe was used
- Block the IP address that is sending the packets
- Tell the ISP through which the packets are being sent

Logging and notification are crucial to an effective network security policy. Together, they make it possible to monitor your network security, identify attacks and attackers, and to address security threats and challenges.

You can install the Log Server on the computer you are using as a management station. Or, you can install the log server software on a different computer using the WatchGuard System Manager installation program and selecting to install only the Log Server component. To add other log servers, see the Configuration Guide for your version of appliance software.

Note

If you install the Management Server, Log Server, or WebBlocker Server on a computer with a desktop firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to change their configuration. See "Installing WatchGuard Servers on computers with desktop firewalls" on page 8 for more information.

Setting Up the Log Server

The Log Server collects logs from each WatchGuard® Firebox®.

Note

Firebox devices with WatchGuard Firebox System version 7.4 or earlier can send log messages to a WatchGuard System Manager 8.0 Log Server or to a WatchGuard Security Event Processor 7.3 or earlier. But, Fireboxes with Fireware appliance software cannot send log messages to a WatchGuard Security Event Processor 7.3 or earlier.

1 On the desktop of the computer that has the Log Server, select the Log Server icon from the WatchGuard toolbar.

The **WatchGuard Log Server Configuration** dialog box appears.

2 Type the encryption key to use for the secure connection between the Firebox and the log servers. For more information about configuring logging, see "Setting Up Your Firebox" in the Configuration Guide for your version of appliance software.

Log Server encryption keys are a minimum of eight characters. The first time you connect to a log server, the default log encryption key is the status passphrase you set when you used the Quick Setup Wizard on your management station.

3 Confirm the encryption key.

4 Select a directory to keep all logs, reports, and report definition files.

5 Click **OK**.

6 Click **Start > Control Panel**. Go to Power Options. Select the **Hibernate** tab and disable hibernation. This is to prevent the Log Server from shutting down when the computer hibernates.

7 To add more Log Servers, see "Setting Up Your Firebox" in the Configuration Guide for your version of appliance software.

Changing the Log Server encryption key

To change the encryption key on the Log Server:

1 Right-click the Log Server icon on the WatchGuard toolbar and select **Status/Configuration**.

2 Select **File > Set Log Encryption Key**.

3 Type the new log encryption key two times.

4 Click **OK**.

Setting Global Logging and Notification Preferences

To see the Log Server status and configuration, right-click the Log Server icon on the WatchGuard toolbar and select **Status/Configuration**. The status and configuration information appears. There are three control areas:

Log Files tab
: To set the options for rolling your log file.

Reports tab
: To schedule regular reports of log entries.

Notification tab
: To control notification.

Together, these controls set the general configuration for events and notifications.

Log file size and rollover frequency

You can control the log rollover by size or by time. When this rollover occurs, the Log Server closes the current log file and opens a new log file. The closed log file can be used for reports, or copied or moved to a different archive location.

To find the best rollover size for your company, you must look at:

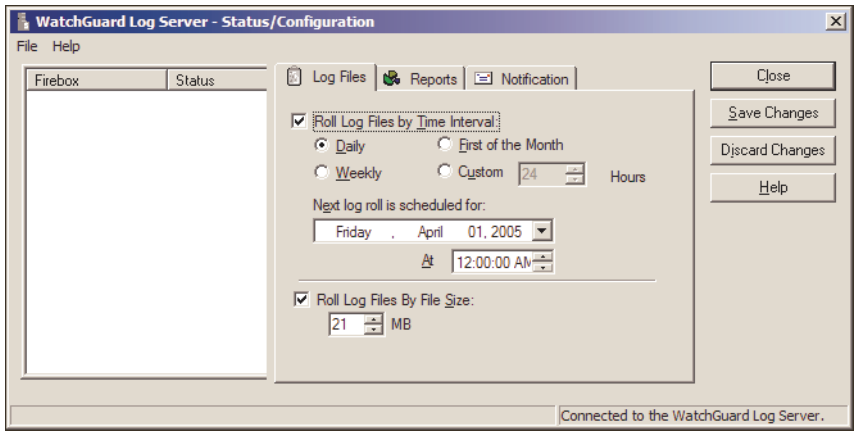
- Storage space that is available
- Number of days you want available
- Size that is best to keep, open, and view
- Number of event types that are recorded
  For example, a small company can get 10,000 entries in two weeks, and a large company with many policies enabled can easily have 100,000 entries in a day.
- Traffic the Firebox processes
- Number of reports to create
  To create a week report, it is necessary to have 8 or 9 days of data. This data can be found in more than one log file, if the log files are in the same location.

It is good to monitor the new log files and adjust the configuration as necessary.

Setting the interval for log rollover

You can control when the log files rollover in the **Log Files** tab in the Log Server configuration interface. You can also manually start a rollover of the current log file by selecting **File > Roll** current log file from the Status/Configuration window.

1 Click the **Log Files** tab.



2 To roll the log file on a time interval, select the **Roll Log Files By Time Interval** check box. Set the time interval. From the **Next Log Roll is Scheduled For** drop-down list, select a date when the log file rolls.

3 To roll the log file based on the size of the log file, select the **Roll Log Files By File Size** check box. Type the maximum size for the log file before the file rolls, or use the spin control to set the number.

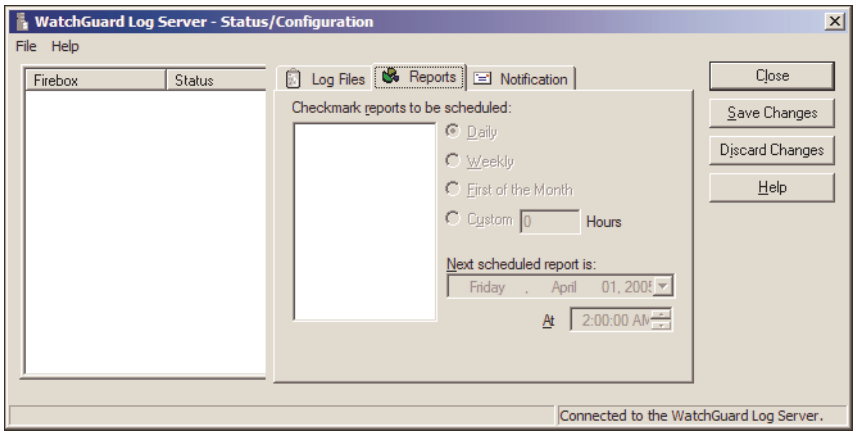
4 Click **Save Changes** or **Close**.

The Log Server interface closes and saves your entries. The new configuration starts immediately. The Log Server restarts automatically.

Scheduling log reports

If you have created network activity reports using Historical Reports, you can schedule the Log Server component to automate the reports. You must first create a report in Historical Reports, or it will not appear in the Log Server interface.

1 Click the **Reports** tab.



2 Use the radio buttons to set the time interval for reports: daily, weekly, first day of the month, or at a custom time.

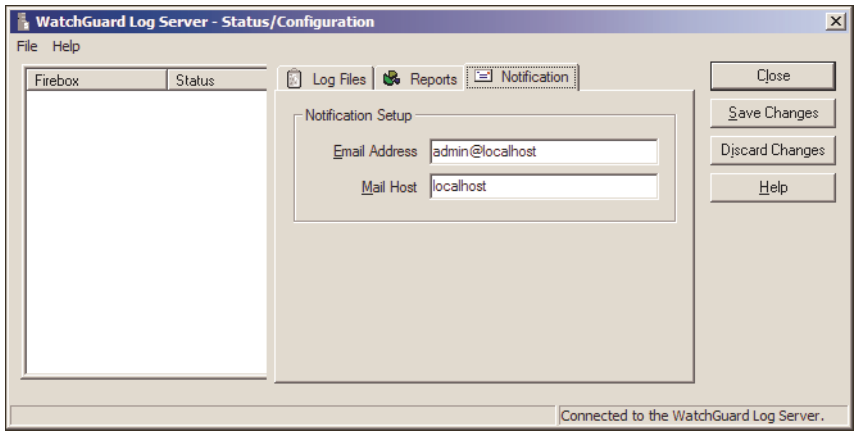
3 From the **Next Scheduled Report** drop-down list, select a date and time for the subsequent scheduled report.

4 Click **Save Changes**.
The Log Server restarts automatically.

Controlling notification

You can configure the Firebox to send an e-mail message when a specified event occurs. Use the **Notification** tab to configure the destination e-mail address. See your Configuration Guide for information about configuring notifications.

1 Click the **Notification** tab.



2 Type the e-mail address and the mail host for notification e-mail messages. Click **Save Changes**.

Starting and stopping the Log Server

You can manually stop or start the Log Server:

- To start the Log Server, right-click the Log Server icon on the toolbar and select **Start Service**.
- To stop the Log Server, right-click the Log Server icon on the toolbar and select **Stop Service.**

CHAPTER 5

Reviewing and Working with Log Files

WatchGuard® System Manager includes strong and flexible log message tools. An important feature of a good network security policy is to log messages from your security systems, to examine those records frequently, and to keep them in an archive. You can use logs to monitor your network security, identify any security risks, and address them.

The WatchGuard Firebox X Core and Firebox X Peak send log messages to a shared log management system called the Log Server. They can also send log messages to a Syslog server or keep logs locally on the Firebox. It is your decision to send logs to any or all of these locations.

You can use Firebox System Manager to log messages in the **Traffic Monitor** tab. For more information, see the *Configuration Guide*. You can also examine log messages with LogViewer. The log messages are kept in an XML file with a .wgl.xml extension in the WatchGuard directory on the log server. You can open this file using any XML editing tool to see full log messages.

Types of Log Messages

The Firebox® sends four types of log messages. Log messages created with Fireware appliance software include the name of the log type in each log message. Log messages created with WFS appliance software give the same data, but do not include the log type category name in the body of the message.

- Traffic
- Alarm
- Event
- Diagnostic

Traffic log messages

The Firebox sends traffic log messages as it applies packet filter and proxy rules to traffic that goes through the Firebox.

Alarm log messages

Alarm log messages are sent when an event occurs that triggers the Firebox to do a command. When the alarm condition is matched, the Firebox sends an Alarm log message to the Traffic Monitor and log server and then it does the specified action.

You can set some alarm log messages. For example, you can use Policy Manager to configure an alarm to occur when a specified value matches or is more than a threshold. Other alarm log messages are set by the appliance software, and you cannot change the value. For example, the Firebox sends an alarm log message when a network connection on one of the Firebox interfaces fails or when a Denial of Service attack occurs. For more information about alarm log messages, see the Reference Guide.

There are eight categories of alarm log messages: System, IPS, AV, Policy, Proxy, Counter, Denial of Service, and Traffic. The Firebox does not send more than 10 alarms in 15 minutes for the same conditions.

Event log messages

The Firebox sends an event log messages because of user activity. Actions that can cause the Firebox to send an event log message include:

- Firebox start up and shut down
- Firebox and VPN authentication
- Process start up and shut down
- Problems with the Firebox hardware components
- Any task done by the Firebox administrator

Diagnostic log messages

Diagnostic log messages include information that you can use to help troubleshoot problems. There are 27 different product components that can send diagnostic log messages. Using Policy Manager, you can select the level of diagnostic log messages to see in your Traffic Monitor or write your log file. For information on how to do this, see the *Configuration Guide* for your appliance software.

Log File Names and Locations

The Firebox® sends log messages to a primary or backup Log Server. The default location for the log file is path: My Documents\My WatchGuard\Shared WatchGuard\logs.

The name of the log file shows:

- If the Firebox has a name, the format of the log file name is `FireboxName-date.wgl.xml`.
- If the Firebox does not have a name, the name of the log files is `FireboxIP-date.wgl.xml`.

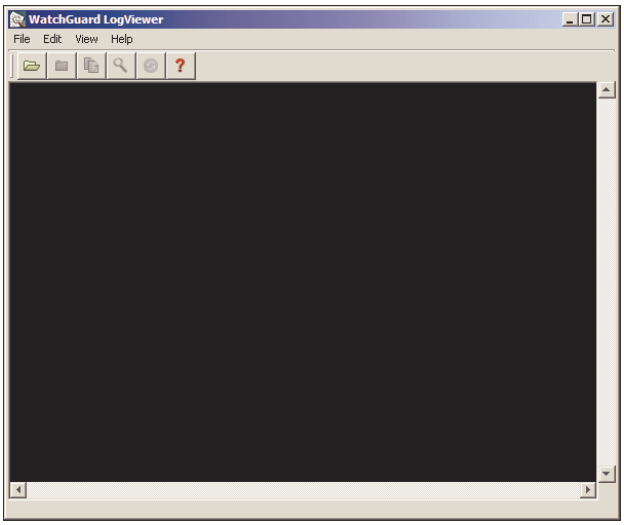
Starting LogViewer

LogViewer is the WatchGuard® System Manager tool you use to see the log file data. It can show the log data page by page, or search and display by key words or specified log fields. The LogViewer tool is the same for Fireware and WFS appliance software. There are small differences between the two appliance

software versions for LogViewer settings and search functions. There is more information about these differences below.

1 From WatchGuard System Manager, select **Resources > LogViewer.**

or
Click the LogViewer icon on the WatchGuard System Manager toolbar. The icon is shown at the left.

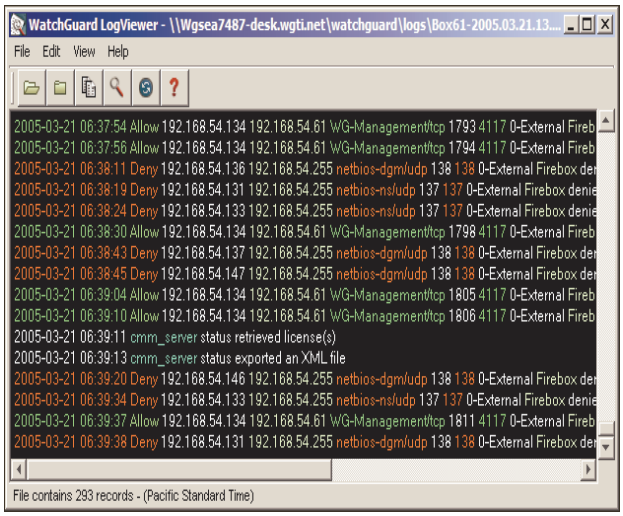


2 From LogViewer, select **File > Open.**

or
Click the Open File icon on the LogViewer toolbar. The icon is show at the left.

The default location of the logs is the path: My Documents\My WatchGuard\Shared Watchguard\logs.

3 Browse to find the log file and click **Open.**
LogViewer shows the log file you selected. A sample appears below.

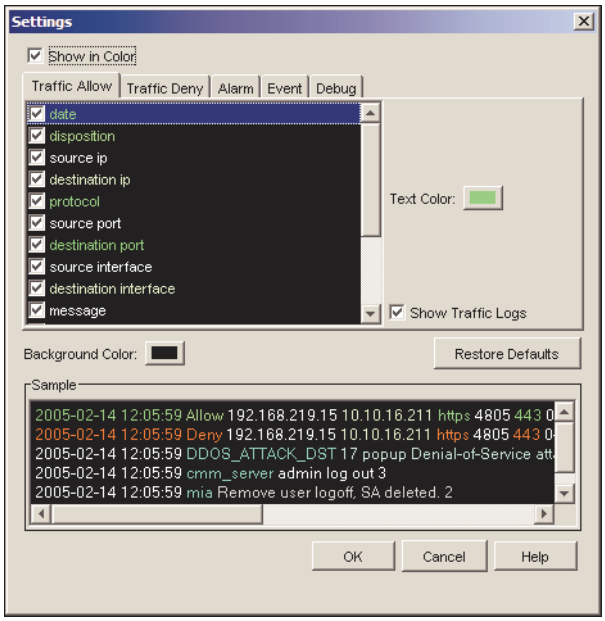


LogViewer Settings

You can adjust the content and the format of the LogViewer window.

Changing LogViewer settings with Fireware appliance software

1 From LogViewer, select **View > Settings**.
The Settings dialog box appears.



The **Settings** dialog box has five tabs, each with the same fields. You use these tabs to set properties for the four types of messages that appear in log files: Alarms, Traffic, Event, and Diagnostic.

Show Logs in Color
You can set the messages to appear in different colors based on the type of log message. If color is not enabled, log messages appear as white text on a black background.

Show Columns
For each type of log message, you can select which columns to show in the LogViewer window. Select the check box adjacent to each field to make it appear.

Text Color
Click **Text Color** to set the color for each type of log message.

Background Color
You can set the background color. If the background and text are the same color, you cannot see the text.

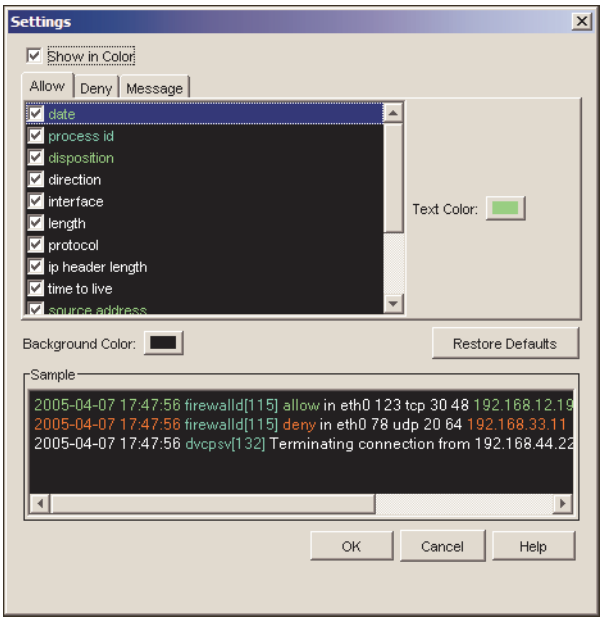
Reset Defaults
Click to set the format of the log messages to the default colors.

Sample
Shows a sample log message with format changes.

Show logs
This check box is on each tab. If the check box is selected on a tab, the log messages for that type of log are included in the LogViewer display. To clear one type of log message from the display, clear the check box on the tab that matches the log type.

Changing LogViewer settings with WFS appliance software

1 From LogViewer, select **View** > **Settings.**
The Settings dialog box appears.



2 From here, you can set the properties for the display of the log messages. Select the tab to configure the display properties for allowed traffic, denied traffic, or other log messages that do not apply to Firebox traffic.

Show Logs in Color

You can set the messages to appear in different colors. If color is not enabled, logs appear as white text on a black background.

Show Columns

For each log message, you can select which columns to show in the LogViewer window. Select the check box adjacent to each field to show.

Text Color

*Clic*k Text Color to set the color of the text of the log message.

Background Color

You can set the background color. If the background and text are the same color, the text does not show.

Reset Defaults

Click to set the format of the logs to the default colors.

Sample

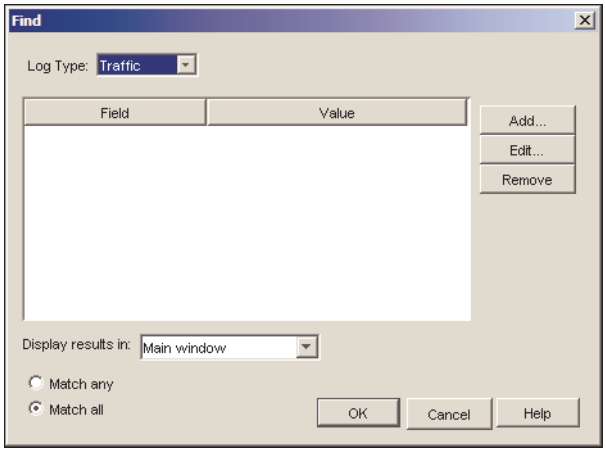
Shows a sample log message with format changes.

Using LogViewer

Creating a Search Rule

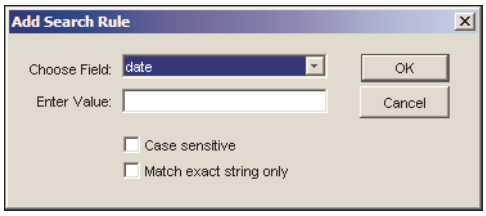
You can create rules to search through the data shown in LogViewer.

1 **Select Edit > Find.**
The Find dialog box appears.



2 Use the **Log Type** drop-down list to select the type of log message to apply the search rule to. You can select: Alarm, Traffic, Event, Diagnostic (debug), or All. If you using the LogViewer to show log messages from a Firebox with WFS appliance software, you cannot select the type of log message.

3 Click on the **Field column** header and select **Add.**
The Add Search Rule dialog box appears.



4 In the **Choose Field** drop-down list, select the field to search.

5 In the **Enter Value** text box, type the text or value to search for.

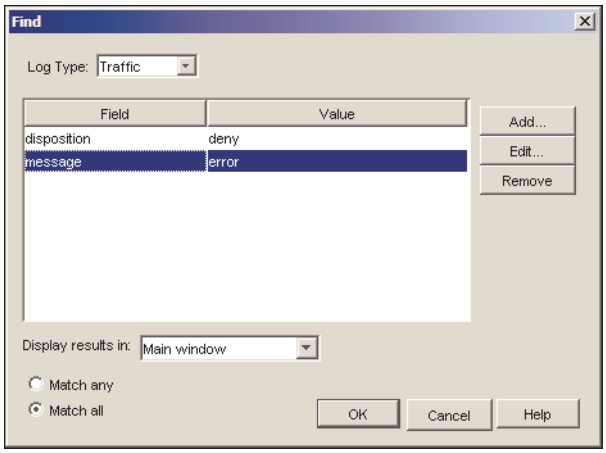
6 If the text you typed in the **Enter Value** text box is case-sensitive, select the **Match Case** check box. To find only entries that match the value precisely, select the **Match exact string only** check box.

7 Click **OK.**

Searching in LogViewer

After you make a search rule, you can use it to search the data shown in LogViewer.

1 If it is necessary to search through log messages from a Firebox using Fireware Pro, use the **Log Type** drop-down list to select which type of log messages appears in the window.



2 Use the **Display Results in** drop-down list to select the method to show the results of the search. The options are:

- *Highlight in main window* — The LogViewer window shows the same log message set, but changes the color of log messages that match the criteria. Use the F3 key to move through specified entries.
- *Main window* — Only the log messages that match the search criteria appear in the primary LogViewer window.
- *New window* - A new window opens to show log messages that match the search criteria.

3 Select from the option:

- *Match any* — Show log messages that match any of the search criteria.
- *Match all* — Show only log messages that match all of the search criteria.

4 Click **OK** to start the search.

Viewing the current log file in LogViewer

You can open the current log file in LogViewer to examine the logs as they are written to the log file. LogViewer automatically updates its display with new log messages at 15-second intervals. If you have a LogViewer search window open with the current log file, it also updates every 15 seconds.

Copying LogViewer data

You can copy log file data from LogViewer to a different tool. Use **copy** to move specified log messages to a different tool.

1 Select the log messages to copy.
Use the Shift key to select a group of entries. Use the Ctrl key to select more than one entry.

2 Select **Edit > Copy**.

3 Paste the data into any text editor.

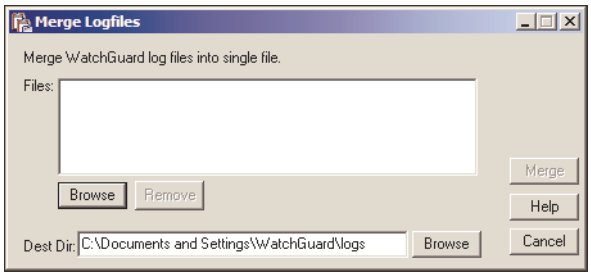
Consolidating log files

You can put together two or more log files into one file. You can then use this file in Historical Reports, LogViewer, or some other tool to examine log data for an extended time interval. To merge more than one log file into one file:

- The log files must be from the same Firebox
- The log messages in the files must be in date and time order
- The log files must be have been created with the same appliance software. You cannot merge a log file created with WFS appliance software with a log file created with Fireware appliance software, even if they are from the same Firebox.

Right-click the Log Server icon on your Windows toolbar and select **Merge Log Files**. Or, from the Log Server Status/Configuration interface:

1 Click **File > Merge log files.**
The Merge Logfiles dialog box appears.



2 Click **Browse** to find the files to put together.

3 Click **Merge**.
The log files are put together and saved to a new file in the specified directory.

Updating .wgl log files to .xml format

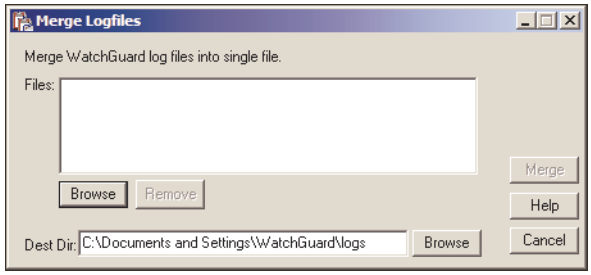
When you migrate from an earlier version of WatchGuard System Manager to WSM 8.0 you can convert log files from .wgl to .xml format. This is also helpful if you manage a mixed network with different versions of WSM. After converting, you can use your WSM 8.0 LogViewer or report tools on log files created with WatchGuard Management System 7.3 or earlier.

When you convert a log file from .wgl to .xml:

- The XML file is usually smaller than the .wgl file. This is because XML log records are variable in length.
- If you open the new XML file in an XML editor, you can see some duplicate entries. This is a function of the way Historical Reports made reports in WSM 7.3 and earlier. It does not cause problems in LogViewer or in Historical Reports for WSM 8.0.

To convert a log file from .wgl to .xml:

1 Right-click the Log Server icon on your Windows desktop tray and select **Merge Log Files.**
The Merge Logfiles dialog box appears. This dialog box controls merges, and also updates, of log files.



2 Click **Browse** to find the location of the logfile.wgl to convert to XML. If you select more than one log file at one time, the utility converts all of the files you select and puts them together into one file. The new file has an .xml format.

3 Click **Merge.**
The utility converts the log file and saves it to the specified folder.

CHAPTER 6

Generating Reports of Network Activity

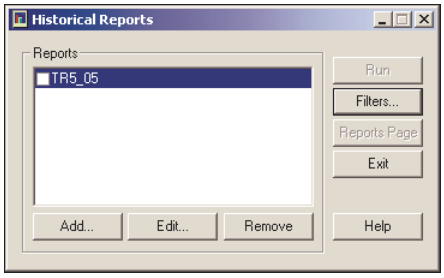
Historical Reports is a tool that makes summaries and reports of the Firebox® log file. You can use these reports to learn about Internet use. You can also measure bandwidth and see which users and software applications use the most bandwidth. Historical Reports creates reports from the log files that are recorded on the WatchGuard® Log Server.

With the advanced features of Historical Reports, you can:

- Set a specified time period for a report.
- Customize the report with data filters.
- Consolidate different log files to create a report for a group of Fireboxes.
- Show the report data in different formats.

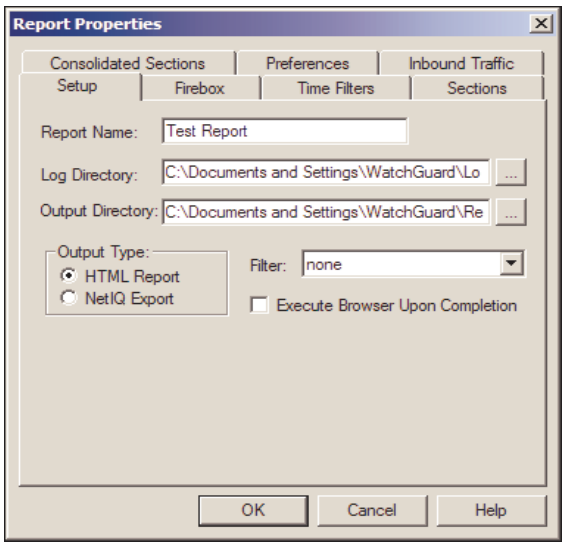
Creating and Editing Reports

To start Historical Reports, click the Historical Reports icon. Or, select **Resources** > **Historical Reports**.



Starting a new report

1 From Historical Reports, click **Add**.
The Report Properties dialog box appears.



2 Type the report name.
The report name appears in Historical Reports and in the name of the output file.

3 Use the text box in the **Log Directory** to give the location of the log files.
The default location for the log files is the path: My Documents\My WatchGuard\Shared WatchGuard\logs.

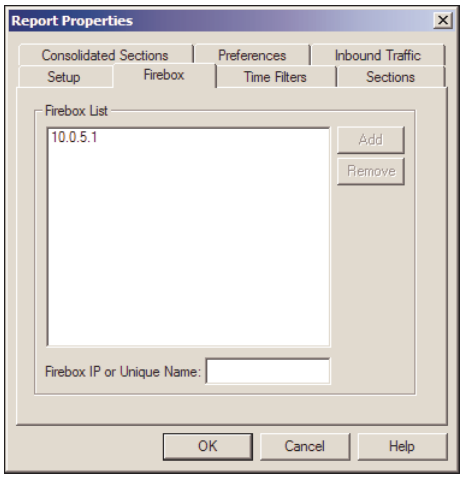
4 Use the text box in the **Output Directory** to give the location of the output files.
The default location for the output files is My Documents\My WatchGuard\Shared WatchGuard\reports.

5 To select the output type, click **HTML Report** or **NetIQ Export**.
For more information on output types, refer to "Exporting Reports" on page 52.

6 Select the filter.
For more information on the filters, refer to "Using Report Filters" on page 53.

7 To see the first page when you use the HTML output, select the **Execute Browser Upon Completion** check box.

8 Click the **Firebox** tab.



9 Type the Firebox® IP address or host name. Click **Add**.
When you type the IP addresses, type all the numbers and the periods. Do not use the TAB or the arrow key. When you create a report with consolidated sections, you must use only WFS Fireboxes or Fireboxes using Fireware Pro. If you use the two Firebox versions in a report the results are not correct.

10 Use the other tabs to specify the report preferences. You can find information about this in the subsequent sections of this chapter.

11 Complete the report configuration. Click OK.
The name of the report appears in the list of the reports.

Editing an existing report

You can always change the definition of a report.

1 From Historical Reports, select the report to change. Click **Edit**.
The Report Properties dialog box appears.

2 Change the report definition.
To see the function of each item, right-click it, and then click What's This?.

Deleting a report

To remove a report from the list of available reports, click on the report. Click **Remove**. This removes the <report name>.`rep` file from the `report-defs` directory.

Viewing the reports list

To see all the reports, click the Reports page. The reports appear in your default browser. You can move through all the reports in the list.

Specifying a Report Time Interval

When you create a Historical Report, the report includes data from the full log file, unless you change the time interval. On the **Time Filters** dialog box, use the drop-down list to select a time interval, for example "yesterday" or "today." You can also manually configure the start and end time. Thus the report uses only the specified time interval:

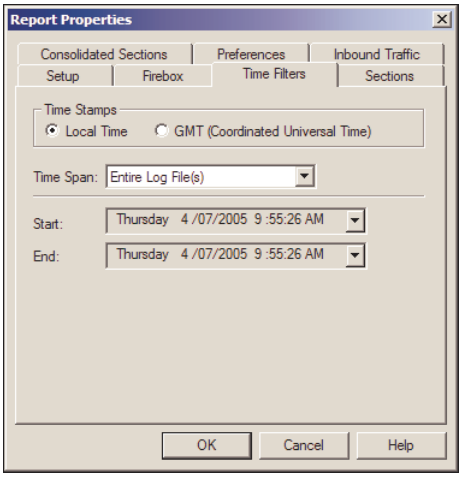
1 In the **Report Properties** dialog box, click the **Time Filters** tab.

2 Select the time-stamp to appear on your report: **Local Time** or **GMT**.

3 From the **Time Span** drop-down list, select the time interval for the report.

4 If you did not select **Specify Time Filters**, click **OK**. If you did select **Specify Time Filters**, click the **Start** and the **End** drop-down lists and select a start and an end time.

5 Click **OK.**



Specifying Report Sections

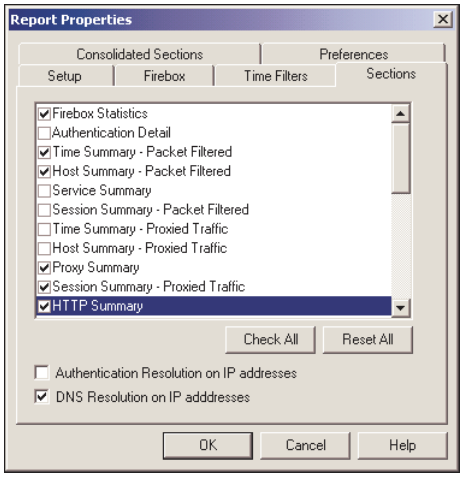
You can select the information to show in the report using the **Sections** tab on the **Report Properties** dialog box.

1 From Historical Reports, click the **Sections** tab.

2 Select the check boxes for the sections to include in the report.
To see the contents of each section, refer to the "Report Sections and Consolidated Sections" on page 54.

3 (Optional) Select the **Authentication Resolution on IP addresses** check box.
You must have user authentication enabled to create reports with resolution from IP address to user name. More time is necessary to create a report with resolution enabled.

4 To use DNS resolution on the IP addresses, select the **DNS Resolution on IP addresses** check box.



Consolidating Report Sections

In the **Sections** tab you can select which information to include in a report. You can get:

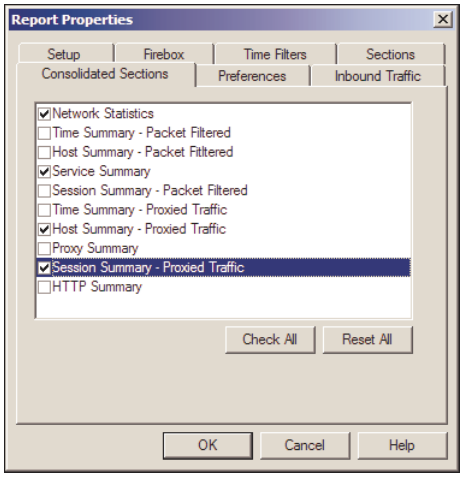
- A vertical look at the data, on each of a group of Fireboxes
- A horizontal or cumulative look at the data, put together for a group of Fireboxes®.

To consolidate report sections:

1 In the **Report Properties** dialog box, select the **Consolidated Sections** tab.
The tab has a list of report sections that you can put together. For short notes of the contents of these sections, refer to "Report Sections and Consolidated Sections" at the end of this chapter.

2 Select the check boxes adjacent to the sections to include in the report. Clear the check boxes for the sections to not include.

3 Click **OK.**



Setting Report Properties

Reports can have Summary sections or Detail sections. You can control the display of each section independently to best show the information that is important to you. A report summary section shows text and graphs containing user-defined information.

To set the report properties:

1 From the **Report Properties** dialog box, select the **Preferences** tab.

2 Type the number of data points (items) to show as a graph in the report.
As an example, if you have 45 hosts, graph the top 10 and list the remaining hosts as "other". The default number is 10.

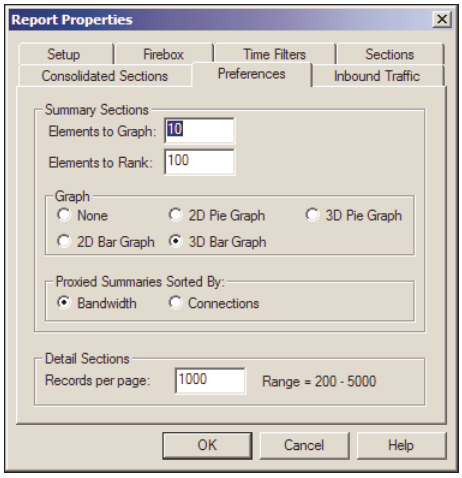
3 Type the number of items to put in the table.
The default number is 100.

4 Select the type of graph to use in the report.

5 Select how to sort the proxied summary: by bandwidth or by connections.

6 Type the number of records to show on each page of the detail sections.
The default number is 1,000 records.

7 Click **OK**.

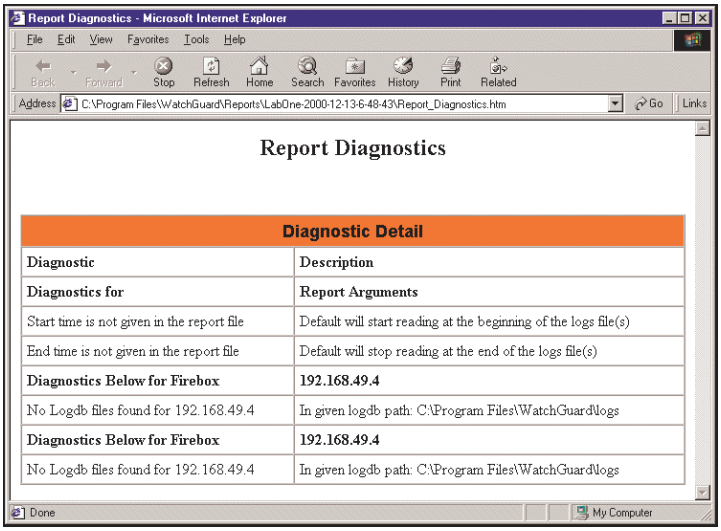


Exporting Reports

You can export a report to two formats: HTML and NetIQ. You can find all reports in the path `c:documents and settings\watchGuard\reports\WebTrends\<export file>`. In the Reports directory are the subdirectories with the name and the time of each report.

Exporting reports to HTML format

If you select **HTML Report** from the **Setup** tab on the **Report Properties** dialog box, the report output is in HTML. You can go to each report section through a JavaScript menu. For this, you must enable JavaScript on the browser. The figure that follows shows how the report can appear in the browser.



Exporting reports to NetIQ format

NetIQ is a leading provider of system and security management solutions. NetIQ supplies full reports about how the Internet is used by an organization, but measures data differently than WatchGuard® His-

torical Reports. To calculate Internet use report data, Historical Reports counts the number of HTTP protocol transactions. NetIQ calculates the number of URL requests.

Note

The WatchGuard HTTP proxy logging must be set to ON to supply NetIQ with the information that is necessary.

You can find the report in:
My Documents\My WatchGuard\Shared WatchGuard\reports

Using Report Filters

A report includes data from the full log file unless you create and use report filters. You can use a report filter to show only data about specified hosts, services, or users. A filter can be one of two types:

Include
: To make a report that includes records with the properties set in the **Host**, the **Service**, or the **User Report Filters** tabs.

Exclude
: To make a report that does not include records with the properties set in the **Host**, the **Service**, or the **User Report Filters** tabs.

You can set a filter to Include or Exclude data in a report with three properties:

Host
: Host IP address

Port
: Service name or port number

User
: Authenticated user name

Creating a new report filter

Use Historical Reports to make a new report filter. You can find the filters in the WatchGuard® installation directory, in the subdirectory `report-defs` with the file extension `.ftr`.

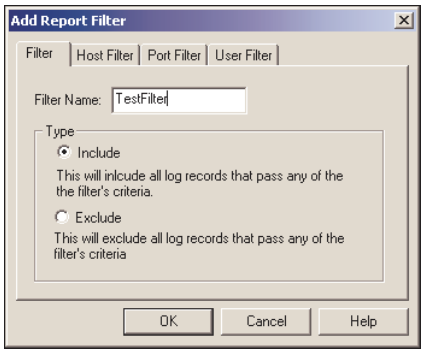
1 From Historical Reports, click **Filters**. Click **Add**.

2 Type the name of the filter. This name appears in the **Filter** drop-down list on the **Report Properties Setup** tab.

3 Select the filter type.
As an example, if you have 45 hosts, graph the top 10 and list the remaining hosts as "other." For a description of include and exclude, see above.

4 Complete the **Filter** tabs.
To see the function of each item, right-click it, and then click What's This?.

5 When finished, click **OK**.
The name of the filter appears in the list of the Filters. The Filter Name.ftr file is in the report-defs directory.



Editing a report filter

You can always change the properties of a filter. From the **Filters** dialog box in Historical Reports:

1 Select the filter to change. Click **Edit**.
The Report Filter dialog box appears.

2 Change the filter properties.
To see the function of each property, right-click it, and then click What's This?.

Deleting a report filter

To remove a filter from the list of filters, select the filter. Click **Delete**. This removes the `.ftr` file from the `\report-defs` directory.

Applying a report filter

Each report can use only one filter. To apply a filter, open the report properties.

1 From Historical Reports, select the report to apply a filter to. Click **Edit**.

2 Use the **Filter** drop-down list to select a filter.
Only if you make a filter in the Filters dialog box will it appear in the drop-down list. For more information, refer to "Creating a new report filter" on page 53.

3 Click **OK**.
Save the new report to the ReportName.rep file in the report-defs directory. When you make the report, the filter is applied.

Running Reports

You can create one or more reports with Historical Reports.:

1 From Historical Reports, select the check box adjacent to each report that is necessary.

2 Click **Run**.

Report Sections and Consolidated Sections

You can use Historical Reports to create a report with one or more sections. Each section includes a different type of information or network traffic. You can put together specified sections to create a summary. You can then create a report on the event log messages of a group of Fireboxes®.

Report sections

There are two basic types of Report sections:

- **Summary —** The sections that rank data by bandwidth or connections.
- **Detailed —** The sections that show all traffic and events with no summary graph or rank.

A list of the different types of the report sections and the consolidated sections is shown below:

Firebox Statistics

A summary of the statistics on one or more log files for one Firebox.

Authentication Detail

A list of authenticated users in the sequence of connection time. The text boxes include:

- Authenticated user
- Host
- Start date and start time of the authenticated session
- End time of the authenticated session
- Length of the session

Time Summary — Packet Filtered

A table, and an optional graph, of all the accepted connections that is divided by user-defined intervals and time. The default time interval is each day, but you can select a different time interval.

Host Summary — Packet Filtered

A table, and an optional graph, of the internal and the external hosts that send packet-filtered traffic through the Firebox. The hosts show in the sequence of the volume of bytes or the number of connections.

Service Summary

A table, and an optional graph, of the traffic for each service in the sequence of the connection count.

Session Summary — Packet Filtered

A table, and an optional graph, of the top incoming and outgoing sessions. The sessions show in the sequence of the volume of bytes or the number of connections. The format of the session is: client > server: service. Historical Reports tries to look up the server port with a table to show the service name. If this does not work, Historical Reports shows the port number.

Time Summary — Proxied Traffic

A table, and an optional graph, of all the accepted connections divided by user-defined intervals and in the sequence of the time. The default time interval is each day, but you can select a different time interval.

Host Summary — Proxied Traffic

A table, and an optional graph, of the internal and the external hosts that send traffic with a proxy through the Firebox. The hosts show in the sequence of the volume of bytes or the number of connections.

Proxy Summary

The proxies in the sequence of bandwidth or connections.

Session Summary — Proxied Traffic

A table, and an optional graph, of the top incoming sessions and outgoing sessions. The sessions show in the sequence of the volume of bytes or the number of connections. The format of the session is: client -> server: service. The service shows in all uppercase letters.

HTTP Summary

Tables, and an optional graph, of the top external domains and hosts that users connect to through the HTTP proxy. The domains and the hosts show in the sequence of the byte count or number of connections.

HTTP Detail

Tables for incoming and outgoing HTTP traffic in the sequence of the time stamp. The fields are Date, Time, Client, URL Request, and Bytes Transferred.

SMTP Summary

A table, and an optional graph, of the top incoming and outgoing e-mail addresses in the sequence of the volume of bytes or the number of connections.

SMTP Detail

A table of the incoming and the outgoing SMTP proxy traffic in the sequence of the time stamp. The fields are: Date, Time, Sender, Recipient(s), and Bytes Transferred.

FTP Detail

Tables for incoming and outgoing FTP traffic, in the sequence of the time stamp. The fields are Date, Time, Client, Server, FTP Request, and Bandwidth.

Denied Outgoing Packet Detail

A list of denied outgoing packets, in the sequence of the time. The fields are: Date, Time, Type, Client, Client Port, Server, Server Port, Protocol, and Duration.

Denied Incoming Packet Detail

A list of denied incoming packets, in the sequence of the time. The fields are Date, Time, Type, Client, Client Port, Server, Server Port, Protocol, and Duration.

Denied Packet Summary

In this section there are different tables. Each table shows the data on the host that denied packets. The data has the time of the first and the last try, the type, the server, the port, the protocol, and the number of tries. If there is only one try, the last field has no data.

Denied Service Detail

A list of events in which a user was denied use of a service. This list includes Incoming and Outgoing requests.

WebBlocker Detail

A list of URLs denied because of WebBlocker, in the sequence of time. The fields are Date, Time, User, Web Site, Type, and Category.

Denied Authentication Detail

A list of each denied authentication, in the sequence of the time. The fields are Date, Time, Host, and User.

IPS Blocked Sites

A list of the IPS blocked sites.

Alarms

Available for Fireware Pro users only, this report lists all device alarms and the problem found with each alarm.

AV Summary

A summary of Gateway AntiVirus for E-mail actions available for Fireware Pro users who subscribe to the antivirus service. The fields include sender, virus detail, if the virus was cleaned, and attachment size of the e-mail.

AV Detail

A list of the source, sender, and virus detail for Gateway AntiVirus for E-mail actions. This section is available for Fireware Pro users who subscribe to the antivirus service.

IPS Summary

A summary of Intrusion Protection Service (IPS) actions, showing percentage traffic type, source IP address, and signature category. This section is available for Fireware Pro users who subscribe to the IPS service.

IPS Detail

A list of all Intrusion Protection Service actions, including source, protocol, and signature detail. This section is available for Fireware Pro users who subscribe to the IPS service.

Consolidated sections

Network Statistics

A summary of the statistics on one or more log files for all the Fireboxes that are monitored.

Time Summary — Packet Filtered

A table, and an optional graph, of all accepted connections divided by user-defined intervals and in the sequence of time. The default time interval is each day, but you can select a different time interval.

Host Summary — Packet Filtered

A table, and an optional graph, of the internal and external hosts that send packet-filtered traffic through the Firebox. The hosts show in the sequence of the volume of bytes or the number of connections.

Service Summary

A table, and an optional graph, of the traffic for all services in the sequence of the connection count.

Session Summary — Packet Filtered

A table, and an optional graph, of the top incoming and outgoing sessions. The sessions show in the sequence of the volume of bytes or the number of connections. The format of the session is: client -> server: service. Historical Reports tries to look up the server port with a table to show the service name. If this does not work, Historical Reports shows the port number.

Time Summary — Proxied Traffic

A table, and an optional graph, of all the accepted connections divided by user-defined intervals and in the sequence of the time. The default time interval is each day, but you can select a different time interval.

Host Summary — Proxied Traffic

A table, and an optional graph, of the internal and external hosts that send traffic with a proxy through the Firebox. The hosts show in the sequence of the volume of bytes or the number of connections.

Proxy Summary

The proxies in the sequence of bandwidth or connections.

Session Summary — Proxied Traffic

A table, and an optional graph, of the top incoming sessions and outgoing sessions. The sessions show in the sequence of the volume of bytes or the number of connections. The format of the session is: client -> server: service. The service shows in all uppercase letters.

HTTP Summary

Tables, and an optional graph, of the top external domains and hosts that users connect to through the HTTP proxy. The domains and the hosts show in the sequence of the byte count or the number of connections.

CHAPTER 7

Managing Certificates and the Certificate Authority

When you create a VPN tunnel, you can select from two types of tunnel authentication: shared secrets or certificates. A certificate is an electronic document that contains a public key. The public key verifies that the certificate is legitimate. A Certificate Authority (CA) is a trusted third-party that gives certificates to clients. In WatchGuard® System Manager, the workstation that is configured as the Management Server also operates as a CA. The CA on the Management Server can give certificates to managed Firebox clients when the Management Server creates VPN tunnels.

Certificate Authorities are a component of a system of key creation, key management and certification with the name Public Key Infrastructure (PKI). The PKI supplies certificate and directory services that can create, supply, keep, and when necessary revoke the certificates.

Certificates usually give more security than shared secrets during the authentication procedure.

Public Key Cryptography and Digital Certificates

Public key cryptography is a central component of a PKI. This cryptographic system includes two mathematically related keys, known as an asymmetric key pair. The user keeps one key, the private key, secret. The user can supply the other key, known as the public key, to other users.

The keys in the key pair go together. Only the owner of the private key can decrypt data encrypted with the public key. Any person with the public key can decrypt data encrypted with the private key.

Certificates are used to make sure public keys are valid. Certificates contain a digital signature created with the public key of a CA certificate. The validity of a certificate can be verified by looking at its digital signature.

Certificates have a lifetime that is set when they are created. But certificates are occasionally revoked before the end date and time that was set for their lifetime. The CA keeps an online, current list of revoked certificates. This list is the certificate revocation list (CRL).

PKI in a WatchGuard VPN

To authenticate VPN tunnels with certificates, you must first configure a Management Server. When you configure the Management Server, the CA is automatically activated. Each managed Firebox client

authenticates to the Management Server. The CA makes sure that the managed Firebox clients are authenticated and then gives a certificate to each client. The two managed Firebox clients use the certificates to authenticate the VPN tunnel being created between them.

MUVPN and certificates

Because MUVPN clients are not clients of the Management Server, they authenticate to the Firebox. Use the MUVPN Wizard from Policy Manager to contact the CA and create a certificate for the MUVPN client. Policy Manager creates a package that includes this certificate and two other files.

The Firebox administrator gives each MUVPN user a package of files. Together, these files are the MUVPN end-user profile. Users who authenticate with shared keys receive one .wgx file. Users who authenticate with certificates receive a .wgx file, a .p12 file (which is the client certificate), and a cacert.pem file (which contains the root certificate).

The MUVPN user who authenticates with certificates then opens the .wgx file. The root and client certificates contained in the cacert.pem and the .p12 files are automatically loaded.

For more information on MUVPN, see the MUVPN Administrator Guide.

Managing the Certificate Authority

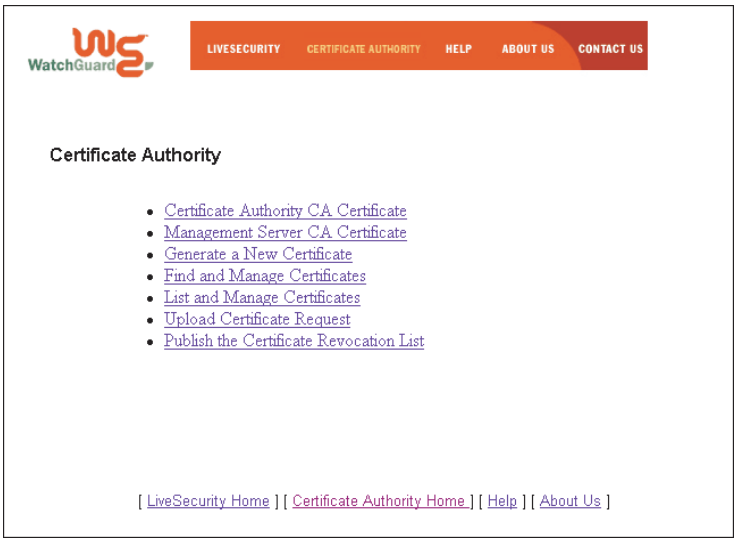
You can control different parameters of the Certificate Authority with the Web-based CA Manager.

1 From WatchGuard System Manager, connect to the Management Server.
You must type the configuration passphrase to connect.

1 Select **Resources > CA Manager**.

or
Click the **CA Manager** icon on the WatchGuard System Manager toolbar. The icon is shown at left.

The menu of the Certificate Authority Settings pages appears.



2 From the menu, select the correct page:

Certificate Authority CA Certificate
Print a copy of the CA (root) certificate to the screen. You can then manually save it to the client.

Management Server CA Certificate

Print a copy of the Management Server CA certificate to the screen. You can then manually save it to the client. You can use this for client access to the authentication Web page.

Generate a New Certificate

Type a subject common name, organizational unit, password, and certificate lifetime to make a new certificate.

- For MUVPN users, the common name must agree with the user name of the remote user.
- For Firebox® users, the common name must agree with the Firebox identifying information (normally, its IP address).
- For a generic certificate, the common name is the name of the user.

Note

Type the organizational unit only if you make certificates for MUVPN users. Do not use this for other types of VPN tunnels. The unit name must appear in this format:
GW:<*vpn gateway name*>
where <*vpn gateway name*> is the value of config.watchguard.id in the configuration file of the gateway Firebox.

Find and Manage Certificates

Give the serial number, common name, or organizational unit of a certificate to find in the database. Also, as an alternative to a special certificate, you can make sure that only active, revoked, or expired certificates are found. The results of the search show on the List Certificates page.

List and Manage Certificates

See a list of certificates that are in the database. Select the certificates to publish, revoke, put back, or remove. For information about how to manage certificates, see the section that follows.

Upload Certificate Request

Use this page to sign a certificate request from a different device. Type in the common name and organizational unit of the subject and select browse to find the CSR (Certificate Signing Request) file.

Publish a Certificate Revocation List (CRL)

Make the CA publish the CRL to all clients with current certificates. A Managed Firebox client cannot create a VPN tunnel if it uses a certificate that is on the CRL to authenticate.

Managing certificates with the CA Manager

You use the List and Manage Certificates page to publish, revoke, put back, or remove certificates:

1 From the List and Manage Certificates page, select the serial number of the certificate to change. The certificate data appears.

2 From the **Choose Action** drop-down list, select one of the subsequent alternatives and then select **GO**:

Publish (PEM)

Publishes the certificate in Privacy Enhanced Mail (PEM) format, which uses a protocol for safe Internet e-mail. This lets you save the certificate to a record and upload it to a third-party unit.

Publish (PKC12)

Publishes the certificate in PKCS12 format. Most Web browsers use this format. This lets you save the certificate to a record and upload it to a third-party unit.

Revoke
Cancels a certificate. Managed Firebox clients will not see that the CRL was revoked until the CRL is published.

Reinstate
Puts back a certificate that was revoked before.

Destroy
Removes a certificate.

CHAPTER 8

Managing the Firebox X Edge and Firebox SOHO 6

WatchGuard® System Manager lets you control and configure WatchGuard firewalls from a distance. This makes for easy configuration and management of a VPN tunnel to a Firebox® X Edge, Firebox S6, Firebox SOHO 6, or Firebox SOHO 5 device. These WatchGuard hardware models are good for small, remote offices.

You configure the WatchGuard small office hardware devices with a Web browser. To increase security while you do this, WatchGuard uses:

- WatchGuard encrypted protocol
- Certificate authentication
- Secure Sockets Layer (SSL)

Note

You must enable certificates on your Web browser. For more information, refer to the online help for your Web browser.

Importing Certificates

When you configure a computer as a Management Server, the WatchGuard® System Manager creates a certificate. The default folder for WatchGuard certificates is:
`C:\Documents and Settings\All Users\Shared WatchGuard\certs.`

From your management station, you must connect to your Management Server. Then, use the steps below to match the type of Internet browser you use on your computer. These steps give instructions to import the certificate into the Web browser on your management station to connect and configure Firebox® small office devices from a distance.

Microsoft Internet Explorer 5.5 and 6.0

If you use Microsoft Internet Explorer 5.5 or 6.0, the certificate is automatically imported for you. To confirm, from the Windows desktop of the management station:

1 Start Internet Explorer. Click **Tools > Internet Options.**
The Internet Options window appears.

2 Click the **Content** tab. Click **Certificates**.
The Certificates window appears.

3 Click the **Personal** tab. You can see the certificate on this tab. If you do not see the certificate in the list, use these troubleshooting ideas to examine the problem:

- Make sure that you have the strong encryption (128-bit) version of Internet Explorer
- Internet Explorer does not always enable strong encryption during the installation. Open the Windows registry and find this key:

  HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Defaults\Provides\001

  This must be Microsoft Enhanced Cryptographic Provider v1.0. If not, edit it manually, and start the browser again.
- Make sure that you have the correct password for the `.p12` (or `.pfx`) file. This must be the configuration passphrase of the Management Server.
- Make sure that the certificate is not zero (0) length. If it is, erase the file and disconnect from System Manager. Open System Manager and make the certificate again.

Netscape Communicator 4.79

From the Windows desktop of the management station:

1 Start Netscape Communicator. Select **Communicator** > **Tools** > **Security Info**.
The Security Info window appears.

2 From the navigation menu on the left side, select **Certificates** > **Yours**.

3 Click **Import a Certificate**.
The File to Import window appears.

4 Browse to the file location, select the certificate, and click **Open**.
The Password Entry Dialog box appears.

5 Type the configuration passphrase of the Management Server and click **OK**.
A window appears that shows that the certificate is correctly imported.

6 Click **OK** to go back to the Certificates window.
The imported certificate appears in the applicable field.

7 Click **OK** to go back to the browser.

Netscape 6

From the Windows desktop of the management station:

1 Start Netscape. Select **Tasks** > **Privacy and Security** > **Security Manager**.
The Netscape Personal Security Manager window appears.

2 Click the **Certificates** tab.

3 From the navigation menu on the left side, click **Mine**.

4 Click **Restore**.
The File Name to Restore window appears.

5 Browse to the file location, select the certificate, and click **Open**.
The Password window appears.

6 Type the configuration passphrase of the Management Server and click **OK**.
A window appears that shows that the certificate is correctly put back.

7 Click **OK** to go back to the Personal Security Manager window.
The imported certificate appears in the applicable field.

8 Click **Close** to go back to the browser.

Troubleshooting ideas

Use these steps to troubleshoot Netscape certificates:

- Make sure that you have the strong encryption (128-bit) version of Netscape.
- Make sure that you have the correct password for the `.p12` (or `.pfx`) file. This must be the configuration passphrase of the Firebox DVCP server.
- Make sure that the certificate is not zero (0) length. If it is, erase the file and disconnect from System Manager. Open System Manager and make the certificate again.

Managing the Firebox X Edge or SOHO Device

After you import the correct certificate in your browser, you can start to use System Manager to connect to a Firebox® X Edge, SOHO 6, or SOHO 5 to monitor and configure it.

You cannot use the same browser window to connect to the Edge or SOHO management pages as the one you use to configure access to the Certificate Authority. You must close the Certificate Authority window before you try to configure an Edge or SOHO from System Manager.

Refer to your Firebox X Edge or Firebox SOHO User Guide for more detailed information about configuring these devices.

From System Manager:

1 Select the Edge or SOHO device. Then click **Policy Manager**.
The Client Authentication dialog box appears.

2 Select the certificate for this device. Click **OK**.

3 Click **OK**.
The SOHO System Status page appears. All management tasks that are usually available locally through a Web browser are available at this time.

System Status

The System Status page is the configuration home page of the Edge or SOHO. The page shows:

- Software appliance version
- Firebox features and their status as Enabled or Disabled
- Upgrade parameters and their status
- Configuration information for the trusted and external networks
- Firewall incoming and outgoing policies
- A reboot button to start the device again

Network

From the Navigation bar on the left side, click **Network** to:

- Configure the device network parameters for the external and trusted networks
- Configure static routes to let traffic through to networks on not connected segments
- Look at network statistics to help to monitor data traffic and troubleshoot problems

Administration

From the Navigation bar on the left side, click **Administration** to:

- Enable System Security passphrases and remote management

- Enable System Manager access
- Update the device from an operating system other than Windows
- Upgrade the device features
- Look at the configuration file as text

System security and remote management

Use this to enable system security, give an administrator name to the device, and set the passphrases.

You can enable the device for remote management. This lets you connect to the unit from a distance with the WatchGuard® Remote Management VPN client. Set the virtual IP address for your remote computer after connection, and the authentication and encryption algorithms to make the connection secure.

Firewall

From the Navigation bar on the left side, click **Firewall** to:

- Configure the incoming and outgoing policies
- Configure blocked sites
- Enable firewall parameters
- Configure a network route to a public server on the optional network

Logging

From the Navigation bar on the left side, click **Logging** to:

- See log messages
- Configure the device to send logs to a WatchGuard Security Event Processor
- Configure the device to send logs to a Syslog server
- Configure the system time

WebBlocker

From the Navigation bar on the left side, click **WebBlocker** to enable and configure this feature. WebBlocker controls users' access to Web sites.

VPN

From the Navigation bar on the left side, click **VPN** to:

- Configure VPN tunnels between the Firebox X Edge or SOHO and other IPSec devices
- Configure MUVPN clients to make Mobile User VPN tunnels to the Edge or SOHO
- See the statistics about active tunnels
- Configure the Keep Alive feature that sends a ping through a VPN tunnel to keep the tunnel from a time-out

Removing Certificates

It could be necessary to update the certificates that System Manager uses. One example is when you change the configuration passphrase of your Management Server. Also, when you install the Management Server again, you must update the certificates. To do this, you must erase the certificates, and then make and use new certificates.

Microsoft Internet Explorer 5.5 and 6.0

From the Windows desktop of the management station:

1. Start Internet Explorer. Click **Tools** > **Internet Options**.
   The Internet Options window appears.
2. Click the **Content** tab. Click **Certificates**.
   The Certificates window appears.
3. Select the certificate or certificates to erase.
4. Click **Remove**.
   A warning window appears.
5. Click **Yes**.
   The selected certificates are erased from the browser.
6. Click **Close** and then click **OK** to go back to the browser.

After you remove the certificates from your browser, you must erase them from your computer.

From System Manager:

- Select **File** > **SOHO Management** > **Clean up on PC**.

Netscape Navigator 4.79

From the Windows desktop of the management station:

1. Start Netscape Communicator. Select **Communicator** > **Tools** > **Security Info**.
   The Security Info window appears.
2. From the navigation menu on the left side, select **Certificates** > **Yours**.
3. Select the certificate or certificates to erase.
4. Click **Delete**.
   A warning window appears.
5. Click **OK**.
   The selected certificates are erased from the browser.
6. Click **OK** to go back to the browser.

After you remove the certificates from your browser, you must erase them from your computer.

- From System Manager, select **File** > **SOHO Management** > **Clean up on PC**.

Netscape 6

From the Windows desktop of the management station:

1. Start the browser and select **Tasks** > **Privacy and Security** > **Security Manager**.
   The Netscape Personal Security Manager window appears.
2. Click the **Certificates** tab.
3. From the navigation menu on the left side, select **Mine**.
4. Select the certificate or certificates to erase.
5. Click **Delete**.
   A warning window appears.
6. Click **Delete**.
   The selected certificates are erased from your browser.
7. Click **Close** to go back to the browser.

After you remove the certificates from your browser, you must erase them from your computer.

- From System Manager, select **File** > **Certificates**. Select the certificate to erase and click **Remove**.

APPENDIX A

Copyright and Licensing

WatchGuard Firebox Software End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:
This Firebox Software End-User License Agreement ("AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD Firebox software product, which includes computer software components (whether installed separately on a computer workstation or on the WATCHGUARD hardware product or included on the WATCHGUARD hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity Service (or its equivalent), (the "SOFTWARE PRODUCT"). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this Agreement. Please read this Agreement carefully. By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, (1) if the SOFTWARE PRODUCT was bundled with a hardware product, promptly return the SOFTWARE PRODUCT and hardware product, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT and hardware product for a full refund of the price you paid or (2) if the SOFTWARE PRODUCT was sold separately, promptly return any license key for the SOFTWARE PRODUCT, along with proof of payment, to (i) the authorized dealer from whom you obtained the SOFTWARE PRODUCT or (ii) if purchased directly from WATCHGUARD, to WATCHGUARD for a full refund of the price you paid. The WATCHGUARD hardware product is subject to a separate agreement and limited hardware warranty included with the WATCHGUARD hardware product packaging and/or in the associated user documentation.

1. Ownership and License. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.

2. Permitted Uses. You are granted the following rights to the SOFTWARE PRODUCT:

(A) You may install and use the SOFTWARE PRODUCT on any single WATCHGUARD hardware product at any single location and may install and use the SOFTWARE PRODUCT on multiple workstation computers.

(B) To use the SOFTWARE PRODUCT on more than one WATCHGUARD hardware product at once, you must purchase an additional copy of the SOFTWARE PRODUCT for each additional WATCHGUARD hardware product on which you want to use it. To the extent that you install copies of the SOFTWARE PRODUCT on additional WATCHGUARD hardware products in accordance with the prior sentence without installing the additional copies of the SOFTWARE PRODUCT included with such WATCHGUARD hardware products, you agree that use of any software provided with or included on the additional WATCHGUARD hardware products that does not require installation will be subject to the terms and conditions of this AGREEMENT. You must also maintain a current subscription to the WatchGuard LiveSecurity Service (or its equivalent) for each additional WATCHGUARD hardware product on which you will use a copy of an updated or modified version of the SOFTWARE PRODUCT received through the WatchGuard LiveSecurity Service (or its equivalent).

(C) In addition to the copies described in Section 2(A), you may make a single copy of the SOFTWARE PRODUCT for backup or archival purposes only.

3. Prohibited Uses. You may not, without express written permission from WATCHGUARD:

(A) Use, copy, modify, merge or transfer copies of the SOFTWARE PRODUCT or printed materials except as provided in this AGREEMENT;

(B) Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;

(C) Sublicense, lend, lease or rent the SOFTWARE PRODUCT;

(D) Transfer this license to another party unless

(i) the transfer is permanent,

(ii) the third party recipient agrees to the terms of this AGREEMENT, and

(iii) you do not retain any copies of the SOFTWARE PRODUCT; or

(E) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to WATCHGUARD with a dated proof of purchase.

(B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and they will provide you with a new version of the SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THE SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ITS LICENSORS AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5.United States Government Restricted Rights. The SOFTWARE PRODUCT is provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Inc., 505 5th Ave. South, Suite 500, Seattle, WA 98104.

6.Export Controls. You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7.Termination. This license and your right to use the SOFTWARE PRODUCT will automatically terminate if you fail to comply with any provisions of this AGREEMENT, destroy all copies of the SOFTWARE PRODUCT in your possession, or voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8.Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the SOFTWARE PRODUCT, and supersedes any prior purchase order, communications, advertising or representations concerning the SOFTWARE PRODUCT AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS AGREEMENT; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AND; (C) THIS AGREEMENT AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of this AGREEMENT will be valid unless it is in writing and is signed by WATCHGUARD.

Version: 050309

Copyright and Trademarks

Patents

U.S. Patent Nos. 6,493,752; 6,597,661; 6,618,755; D473,879. Other Patents Pending.

Licenses

Some components of the WatchGuard System Manager software distribute with source code covered under one or more third party or open source licenses. We include below the full text of the licenses as required by the terms of each license. To get the source code covered under these licenses, please contact WatchGuard Technical Support at:

- 877.232.3531 in the United States and Canada
- +1.360.482.1083 from all other countries

This source code is free to download. There is a $35 charge to ship the CD.

SSL Licenses

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

OpenSSL License

BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Original SSLeay License

This product includes cryptographic sofware written by Eric Young (eay@cryptsoft.com). includes software written by Tim Hudson (tjh@cryptsoft.com).

© 1995-2003 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes' SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2003 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).''
4. The names ''mod_ssl'' must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called ''mod_ssl'' nor may ''mod_ssl'' appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment: ''This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).''
THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Apache Software License, Version 2.0, January 2004

Some components of the WatchGuard System Manager software are distributed with a version of the Apache web server and other source code under the Apache software license.

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include

works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

PCRE License

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. The PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service, Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2004 University of Cambridge All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU Lesser General Public License

Some components of the WatchGuard System Manager software distribute with source code covered under the GNU Lesser General Public License (LGPL).

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system rather than copying library functions into the executable, and (2) operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if

you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

GNU General Public License

Some components of the WatchGuard System Manager software distribute with source code covered under the GNU General Public License (GPL).

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY

GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
END OF TERMS AND CONDITIONS

Sleepycat License

Some components of the WatchGuard System Manager software are distributed with a version of the BerkeleyDB covered under the Sleepycat software license.

Copyright (c) 1990-2004

Sleepycat Software. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Redistributions in any form must be accompanied by information on how to obtain complete source code for the DB software and any accompanying software that uses the DB software. The source code must either be included in the distribution or be available for no more than the cost of distribution plus a nominal fee, and must be freely redistributable under reasonable conditions. For an executable file, complete source code means the source code for all modules it contains. It does not include source code for modules or files that typically accompany the major components of the operating system on which the executable file runs.

THIS SOFTWARE IS PROVIDED BY SLEEPYCAT SOFTWARE ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED. IN NO EVENT SHALL SLEEPYCAT SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1990, 1993, 1994, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY HARVARD AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HARVARD OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Note

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

APPENDIX B

WatchGuard File Locations

This appendix lists the default location of many of the -s used by WatchGuard System Manager.

General File Locations

This table describes the location where data files are stored by the WatchGuard System Manager software. Since it is possible to configure the Windows operating system (OS) to put these directories on different disk drives, you must determine the exact location of these files based on the configuration of Windows on your computer.

It is also possible to configure log files to be kept in a different directory than other installation files. If you change the default location of log files, these default locations do not apply.

If you are using an OS version that is not English, you must translate directory names (such as "Documents and Settings" or "Program Files") to the match the OS language you use.

File Type	Location
User Created Data	C:\Documents and Settings\<username>\My Documents\My WatchGuard (User created data includes files such as Firebox config files, license files, and certificates. In many cases, the WSM software creates subfolders in the My WatchGuard folder to store these files.)
User Created Data (Shared)	C:\Documents and Settings\All Users\Shared WatchGuard
Firebox Configuration Files	C:\Documents and Settings\<username>\My Documents\My WatchGuard\Configs <username> = the Windows username for the current user
Firebox Log Files	C:\Documents and Settings\WatchGuard\logs\
Report Files	C:\Documents and Settings\WatchGuard\reports\

File Type	Location
Certificates	C:\Documents and Settings\All Users\Shared WatchGuard\certs (Except for certificates used by the Log Server, the Management Server, and the Certificate Authority)
WatchGuard Applications	C:\Program Files\WatchGuard\wsm8\
Shared Application Libraries	C:\Program Files\Common Files\WatchGuard\wsm8\
Management Server Data	C:\Documents and Settings\WatchGuard\dvcp\
Certificate Authority Data	C:\Documents and Settings\WatchGuard\wmserver\wgca\
WebBlocker Server Data	C:\Documents and Settings\WatchGuard\
Application Specific Data (Internal Operational Data)	C:\Documents and Settings\<username>\Application Data\WatchGuard\ <username> = the Windows username for the current user
Shared Application Data (Internal Operational Data)	C:\Documents and Settings\All Users\Application Data\WatchGuard\
Future Product Upgrade Images	C:\Program Files\Common Files\WatchGuard\Resources
Help Files (Fireware)	C:\Program Files\WatchGuard\wsm8\help\
Help Files (WFS)	C:\Program Files\WatchGuard\wsm8\wfs\

Default File Locations

These tables describe the default location where the WatchGuard applications and servers will look for their data files or for data files created by users (such as Firebox configuration files). In some cases, the default location changes, depending on the last place the application opened a file of a similar type. In these cases, the application remembers the last place the file was read/written and looks in that location first.

Since it is possible to configure the Windows operating system (OS) to put these directories on different disk drives, you must determine the exact location of these files based on the configuration of Windows on your computer.

It is also possible to configure log files to be kept in a different directory than other installation files. If you change the default location of log files, these default locations do not apply.

If you are using an OS version that is not English, you must translate directory names (such as “Documents and Settings” or “Program Files” to the match the OS language you use.

Quick Setup Wizard

Operation	File Type	Default Location
Write	Application Log	C:\Documents and Settings\<username>\Application Data\WatchGuard\qswiz.log
Write	Firebox Config File	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\<fb-name_wizard>.xml

Quick Setup Wizard

Write	License File	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\<fb-name_wizard>.tgz
Read	License File	C:\Documents and Settings\<username>\My Documents\My WatchGuard\

Firebox System Manager for Fireware Appliance Software

Operation	File Type	Default Location
Read	Application Config File	C:\Documents and Settings\All Users\Application Data\WatchGuard\fsm.conf
Read/ Write	Preferences File	C:\Documents and Settings\<username>\Application Data\WatchGuard\fsm_preference
Write	Application Log File	C:\Documents and Settings\<username>\Application Data\WatchGuard\fsm.log
Write	Support Log File	C:\Documents and Settings\<username>\My Documents\My WatchGuard\<ip-addr>
Read	Help Files	C:\Program Files\WatchGuard\wsm8\help\fsm_help_map.csv

HostWatch for Fireware Appliance Software

Operation	File Type	Default Location
Write	Application Log File	C:\Documents and Settings\<username>\Application Data\WatchGuard\fsm.log
Read/ Write	Preferences File	C:\Documents and Settings\<username>\Application Data\WatchGuard\fsm_preference
Read	Help Files	C:\Program Files\WatchGuard\wsm8\help\fsm_help_map.csv

Policy Manager for Fireware Appliance Software

Operation	File Type	Default Location
Read/ Write	Firebox Backups	C:\Documents and Settings\All Users\Shared WatchGuard\backups\
Read	Product Upgrade Images	C:\Program Files\Common Files\WatchGuard\Resources\
Read	DVCP/CA Cert	C:\Documents and Settings\All Users\Shared WatchGuard\certs
Read	Dynamic Routes (RIP, OSPF, BGP)	C:\Documents and Settings\<username>\My Documents\My WatchGuard\

Policy Manager for Fireware Appliance Software

Operation	File Type	Default Location
Read	Blocked Sites	C:\Documents and Settings\<username>\My Documents\My WatchGuard\
Read	Blocked Sites Exceptions	C:\Documents and Settings\<username>\My Documents\My WatchGuard\
Read/ Write	Firebox Config Files	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\
Read/ Write	Firebox License Files	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\
Read	Initial License Import	C:\Documents and Settings\<username>\My Documents\My WatchGuard\
Write	MUVPN .wgx File	C:\Documents and Settings\All Users\Shared WatchGuard\muvpn\
Read	Help Files	C:\Program Files\WatchGuard\wsm8\help\pm_help_map.csv

WatchGuard System Manager

Operation	File Type	Default Location
Read	Config File	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\
Write	Management Server Config File	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\
Write	CA Admin Cert	C:\Documents and Settings\All Users\Shared WatchGuard\certs\<IP ADDRESS OF DVCP>
Write	SOHO Admin Cert	C:\Documents and Settings\All Users\Shared WatchGuard\certs\<IP ADDRESS OF DVCP>
Write	CA Client Cert	C:\Documents and Settings\All Users\Shared WatchGuard\certs\<IP ADDRESS OF DVCP>
Read	Help Files	C:\Program Files\WatchGuard\<product>\wfs\help

Policy Manager for WFS Appliance Software

Operation	File Type	Default Location
Read	Logging Notification	Current Working Directory
Read	Spam Rules Import	Current Working Directory

Policy Manager for WFS Appliance Software

Operation	File Type	Default Location
Write	Save Backup	C:\Documents and Settings\All Users\Shared WatchGuard\backups\
Read/ Write	Firebox Config Files	C:\Documents and Settings\<username>\My Documents\My WatchGuard\configs\
Write	MUVPN SPDs	C:\Documents and Settings\All Users\Shared WatchGuard\muvpn\
Read	Blocked Sites Import	Current Working Directory
Read	Help Files	C:\Program Files\WatchGuard\wsm8\wfs\

Firebox System Manager for WFS Appliance Software

Operation	File Type	Default Location
Read	Help Files	C:\Program Files\WatchGuard\<product>\wfs\help\

HostWatch for WFS Appliance Software

Operation	File Type	Default Location
Read	Firebox Log File	C:\Documents and Settings\WatchGuard\logs\
Read	Help Files	C:\Program Files\WatchGuard\wsm8\wfs\help\

Flash Disk Management for WFS Appliance Software

Operation	File Type	Default Location
Read/ Write	Backup Image	C:\Documents and Settings\All Users\Shared WatchGuard\backups\
Read	Help Files	C:\Program Files\WatchGuard\wsm8\wfs\help\

LogViewer

Operation	File Type	Default Location
Read/ Write	Application Config File	C:\Documents and Settings\<username>\Application Data\WatchGuard\
Read	Log4j File	C:\Documents and Settings\<username>\Application Data\WatchGuard\

LogViewer

Operation	File Type	Default Location
Write	Application Log File	C:\Documents and Settings\<username>\Application Data\WatchGuard\logviewer.log
Read	Firebox Log File	C:\Documents and Settings\WatchGuard\logs\
Read	Help File	C:\Program Files\WatchGuard\wsm8\help\

Management Server

Operation	File Type	Default Location
Read/ Write	All Files	C:\Documents and Settings\WatchGuard\wmserver\dvcp\

WebBlocker Server

Operation	File Type	Default Location
Read/ Write	All files	C:\Documents and Settings\WatchGuard\wbserver\

Log Server User Interface

Operation	File Type	Default Location
Read/ Write	Log Server Config File (WFS)	C:\Program Files\WatchGuard\wsm8\wfs\controld.wgc
Write	Log Server Cert	C:\Documents and Settings\WatchGuard\wlserver\certs\wglog.pem
Write	Log Server Cert File (WFS)	C:\Documents and Settings\WatchGuard\wlserver\keys\wglog.pem
Write	Log Server Config	C:\Program Files\WatchGuard\wsm8\wlserver\conf\httpd.conf
Write	Log Server Config	C:\Program Files\WatchGuard\wsm8\wlserver\conf\logserver.conf
Read	Help Files	C:\Program Files\WatchGuard\<product>\wfs\help

Log Server for Fireware Appliance Software

Operation	File Type	Default Location
Read	Log Server Config (Fireware)	C:\Program Files\WatchGuard\wsm8\wlserver\conf\httpd.conf
Read	Log Server Config (Fireware)	C:\Program Files\WatchGuard\wsm8\wlserver\conf\logserver.conf
Read	Cert	C:\Documents and Settings\WatchGuard\wlserver\certs\wglog.pen
Write	Log Server Log	C:\Documents and Settings\WatchGuard\logs\wlserver.log
Read/ Write	Active Firebox Logs	C:\Documents and Settings\WatchGuard\logs\wlserver.ini
Write	Firebox Logs (Fireware)	C:\Documents and Settings\WatchGuard\logs\<appliance>-...

Log Server for WFS Appliance Software

Operation	File Type	Default Location
Read/ Write	Log Server Config File	C:\Program Files\WatchGuard\wsm8\wfs\controld.wgc
Write	Log Server Log	C:\Documents and Settings\WatchGuard\logs\controld.log
Read/ Write	Active Firebox Logs	C:\Documents and Settings\WatchGuard\logs\controld.ini
Read/ Write	Firebox Log Files	C:\Documents and Settings\WatchGuard\logs\
Write	WFS Appliance Config File	C:\Documents and Settings\WatchGuard\logs\<appliance>.wgc
Read	Read/Write Cert File	C:\Documents and Settings\WatchGuard\wlserver\certs\wglog.pem

Historical Reports

Operation	File Type	Default Location
Read/ Write	Report Definitions	C:\Documents and Settings\WatchGuard\report-defs\<report name>.def (xml)
Read/ Write	Report Files	C:\Documents and Settings\WatchGuard\reports\<reportname>\report files\
Read/ Write	Reporting Graphics	C:\Program Files\WatchGuard\wsm8\reports\graphics\<report .jpg/.gif files>
Read	Firebox Logs	C:\Documents and Settings\WatchGuard\logs\<appliance>-...

Historical Reports

Operation	File Type	Default Location
Read/ Write	Report Filters	C:\Documents and Settings\WatchGuard\report-defs\<filtername>.flt
Read	Help Files	C:\Program Files\WatchGuard\<product>\wfs\help\

Log Merge

Operation	File Type	Default Location
Read	Log Files	C:\Documents and Settings\WatchGuard\logs\
Write	Converted Log Files	C:\Documents and Settings\WatchGuard\logs\<appliance>... .wgl to .wgl.xml
Write	Merged Log File	C:\Documents and Settings\WatchGuard\logs\<appliance>...merged-wgl.xml
Read	Help Files	C:\Program Files\WatchGuard\<product>\wfs\help

Management Server Setup Wizard

Operation	File Type	Default Location
Read/ Write	wg.cfg	C:\Documents and Settings\WatchGuard\wmserver\tmp
Read/ Write	wg.cfg.new	C:\Documents and Settings\WatchGuard\wmserver\tmp
Read/ Write	dvcp_config.xml	C:\Documents and Settings\WatchGuard\wmserver\tmp
Read/ Write	wgca_config.xml	C:\Documents and Settings\WatchGuard\wmserver\tmp
Read/ Write	advdvcp.cfg	C:\Documents and Settings\WatchGuard\wmserver\tmp
Read/ Write	dvcp.cfg	C:\Documents and Settings\WatchGuard\wmserver\tmp
Read	dvcpinit.dat	C:\Documents and Settings\WatchGuard\wmserver\conf

Management Server User Interface

Operation	File Type	Default Location
Read	Help Files	C:\Program Files\WatchGuard\wsm8\help

WatchGuard Certificate Authority

Operation	File Type	Default Location
Write	Publish CRL	C:\Documents and Settings\WatchGuard\wmserver\htdocs\wgca.crl
Read/ Write	Manage Certs	C:\Documents and Settings\WatchGuard\wmserver\wgca\index.txt C:\Documents and Settings\WatchGuard\wmserver\wgca\index.txt.attr C:\Documents and Settings\WatchGuard\wmserver\wgca\serial C:\Documents and Settings\WatchGuard\wmserver\wgca\serial_server C:\Documents and Settings\WatchGuard\wmserver\wgca\wgca.cnf C:\Documents and Settings\WatchGuard\wmserver\wgca\wgca.ini C:\Documents and Settings\WatchGuard\wmserver\wgca\wgreq.cnf C:\Documents and Settings\WatchGuard\wmserver\wgca\certs*.pem C:\Documents and Settings\WatchGuard\wmserver\wgca\keys*.pem

Index

Symbols

A

C

D

E

F

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT:
www.watchguard.com/support
support@watchguard.com
U.S. and Canada +877.232.3531
All Other Countries +1.206.613.0456

SALES:
U.S. and Canada +1.800.734.9905
All Other Countries +1.206.521.8340

ABOUT WATCHGUARD

WatchGuard is a leading provider of network security solutions for small- to mid-sized enterprises worldwide, delivering integrated products and services that are robust as well as easy to buy, deploy and manage. The company's Firebox X family of expandable integrated security appliances is designed to be fully upgradeable as an organization grows and to deliver the industry's best combination of security, performance, intuitive interface and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of the security landscape with vulnerability alerts, software updates, expert security instruction and superior customer care. For more information, please call (206) 521-8340 or visit www.watchguard.com.